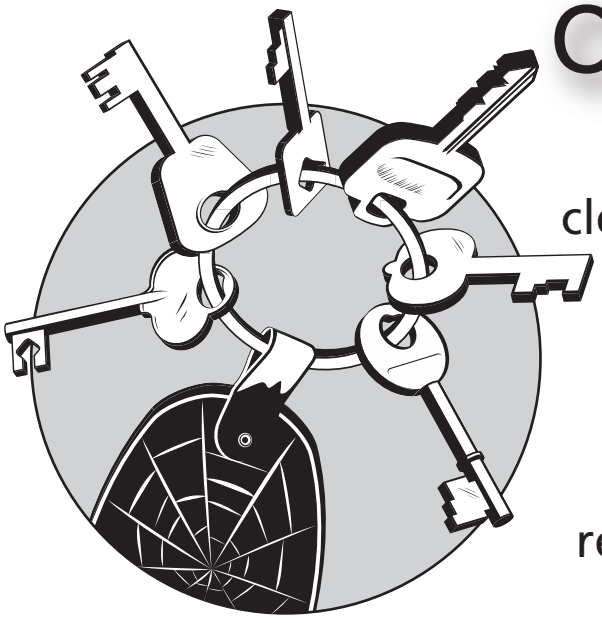
chapitre 2



OpenPGP

clé publique, clé privée

paire de clés

signature

réseau de confiance

Les concepts de base de la norme OpenPGP

Qu'apporte OpenPGP, en termes de sécurité, et en particulier, qu'est-ce que le réseau de confiance qui en est le fondement ?
Quelle différence entre OpenPGP et les certificats électroniques ?
Quelles options et précautions prendre lors de la création d'une paire de clés ?

SOMMAIRE

MOTS-CLÉS

- clé
- paire de clé
- confiance
- signature

Maintenant que vous connaissez les principes de base de la cryptographie, vous vous demandez peut-être ce qui particularise OpenPGP par rapport aux autres systèmes de chiffrement, en dehors des interminables poursuites judiciaires dont a été victime son créateur. Après tout, les techniques cryptographiques sous-jacentes à OpenPGP ont été déployées dans une grande variété d'applications et de protocoles ; ce n'est donc pas cela qui le singularise.

Le secret d'OpenPGP est un concept qui lui est unique : le réseau de confiance, « Web of Trust » en anglais. Pour bien utiliser OpenPGP, vous devez comprendre ce qu'est ce réseau.

Les détails de la gestion du réseau de confiance seront évoqués au chapitre 5 ; PGP sera traité de manière plus spécifique au chapitre 6 et GnuPG au chapitre 7.

Dans ce chapitre, nous verrons les principes de fonctionnement du réseau de confiance. Nous évoquerons aussi quelques considérations à prendre en compte lors de la création et de l'utilisation de clés publiques et privées.

OpenPGP : quelle « sécurité » exactement ?

Réfléchissons un instant aux différents aspects du concept très flou de « sécurité ». En effet, si OpenPGP offre bien certaines solutions dans ce domaine, il ne donne pas une réponse à tous les problèmes qui peuvent se présenter.

OpenPGP n'empêchera personne de voler votre ordinateur, ni de vous envoyer trois millions de messages indésirables. Il permet la confidentialité, l'intégrité et la non-répudiation, mais la mise en œuvre de chacune de ces trois fonctions est fortement liée au concept d'identité.

RAPPEL De la difficulté d'identifier l'autre dans un échange électronique

L'identification d'une personne se trouvant en face de soi ne pose généralement pas de problème : c'est quelque chose que nous faisons depuis des millénaires avec nos cinq sens, et en conséquence, c'est un domaine où nous excellons. Cependant, il en va tout autrement lorsqu'il s'agit d'identifier l'expéditeur d'un message électronique. En effet, la seule information qu'un tel message comporte de son expéditeur est son en-tête, qui est aisément falsifiable.

On peut même dire que l'idée de base d'OpenPGP est la vérification d'identité. En effet, lorsque vous recevez un message signé à l'aide de la clé privée de quelqu'un, vous pouvez être pratiquement certain que l'expéditeur dispose bien de la clé privée correspondante. Le problème qui se pose alors est : comment associer l'identité d'une personne réelle à une paire de clés ? Ce problème a longtemps été l'une des faiblesses de la cryptographie à clé publique.

C'est ici qu'entre en scène le réseau de confiance, dont l'objectif est de permettre de se passer d'une autorité de certification centralisée et de transférer la responsabilité de la vérification d'identité aux mains des utilisateurs.

Référence Comprendre la différence entre PGP et les certificats électroniques

Dans de nombreuses entreprises soucieuses de leur sécurité, on trouve moins souvent PGP que des infrastructures de clés créant pour leurs utilisateurs et serveurs des certificats électroniques. PGP et les certificats électroniques sont-ils concurrents ?

La norme définissant le format de ces certificats électroniques s'appelle X.509 (version 3), en référence à la norme des annuaires, appelée X.500, dont elle est la lointaine héritière. Les certificats, à la norme X.509, ont ceci de commun avec PGP en ce qu'ils partagent les mêmes fonctionnements cryptographiques fondamentaux, en utilisant la techniques des clés asymétriques. Ils assurent donc, techniquement parlant, les mêmes types de garanties électroniques. Ces garanties sont l'authentification forte, la confidentialité, l'intégrité et la non-répudiation, assurées par deux techniques: le chiffrement et la signature électroniques.

Ces deux normes diffèrent cependant sur de nombreux autres points, d'où le sentiment général qu'elles sont «concurrentes».

Première différence, la plus visible peut-être : du point de vue du format, PGP et les certificats sont incompatibles. Un message chiffré avec un système ne peut être lu avec un logiciel qui ne mettrait en œuvre que l'autre technologie.

Au delà de ce simple aspect formel, il y a également un plus grand support de l'industrie informatique pour les certificats électroniques. S'il existe des greffons PGP pour Outlook ou Thunderbird, ces logiciels supportent par ailleurs nativement les certificats, tout comme les routeurs VPN, les clients et les serveur web, beaucoup de système de login comme MS-Gina ou Unix PAM, voire Microsoft Word et OpenOffice.org !

La raison profonde de cette adoption par l'industrie de l'informatique est liée à la troisième différence, déterminante, entre PGP et les certificats. Il s'agit d'une différence de nature, et même de conception, entre PGP et X.509.

- Les certificats sont émis par une infrastructure de gestion de clés, placées entre les mains d'une organisation qui en répond, comme une entreprise ou un gouvernement. Ils sont fondés sur l'idée d'organisation, de structure de référence, dont dépendent les utilisateurs. Ils obéissent à des règles de sécurité simples et transitives : si un utilsateur dispose d'un certificat d'une entreprise Lambda, il fera automatiquement confiance à tous les utilisateurs de certificats Lambda et à tous les serveurs dont les certificats seront signés par Lambda. En d'autres termes, l'utilisateur n'a pas trop de question à se poser : l'organisation « pense » pour lui la sécurité.
- PGP au contraire est fondé sur l'idée d'individu et a été conçu en vue de promouvoir et de défendre les libertés individuelles. C'est l'utilisateur, et non son entreprise ou son gouvernement, qui crée, gère et ordonne ses clés et ses critères de confiance. L'utilisateur crée ses clés et tisse lui-même ses réseaux de confiance, avec ses proches, ses amis, ses connaissances puis les connaissances de connaissances, comme on le verra dans ce livre. Rien ne lui est imposé : il définit précisément ce qu'il fait et à qui il accorde sa confiance.

Il s'agit donc de deux visions du monde radicalement différentes. On serait tenté de résumer ainsi : les certificats seraient le choix des entreprises, des industriels et des puissants, intégrant dans leurs infrastructures la gestion de clés centralisées, ainsi que les moyens pour contrôler les utilisateurs ; PGP à l'opposé serait le hérault vertueux de la liberté individuelle ? Pas si simple.

PGP et X.509 ne sont pas des technologies directement concurrentes en ce qu'elles sont... complémentaires. Tout individu a le droit d'assurer le respect sa vie privée et un outil comme PGP permet l'exercice de ce droit fondamental. Par ailleurs, des organisations ont le droit (et ont intérêt) à assurer la sécurité de leurs échanges et de leurs transactions, et de s'en porter caution, pour les usages dans le cadre de leurs activités, y compris avec des utilisateurs incompétents voire potentiellement hostiles aux mesures de sécurité que l'organisation entend mettre en place.

Les certificats obéissent à une logique régalienne, PGP obéit à une logique individualiste. Ces deux logiques peuvent parfaitement coexister: sphère privée, sphère collective ou publique.

Il est donc tout à fait possible et légitime pour une personne de disposer d'une clé PGP pour ses activités privées ou associatives et de disposer de certificats pour d'autres activités, lorsque ces activités dépendent d'organisations, comme son entreprise ou son gouvernement, comme les certificats inclus dans les cartes de santé, les cartes d'identité (nos lecteurs belges disposent d'une carte d'identité électronique depuis 2003) ou encore les passeports électroniques.

Les entreprises résolvent ce problème en mettant en œuvre les grands moyens. Ainsi, les sites utilisant le protocole sécurisé SSL utilisent-ils des certificats numériques provenant d'Autorités de certification, des sociétés dont la principale fonction est de vérifier l'identité réelle des personnes ou des entreprises qui demandent un certificat pour leur site. Ce processus, lorsqu'il est correctement effectué, prend du temps et coûte cher. Une fois l'identité vérifiée, l'autorité de certification signe numériquement la clé publique du site, ce qui revient pour cette autorité à confirmer qu'elle a vérifié l'identité du détenteur du certificat.

Si cette approche fonctionne globalement très bien, elle n'est pas sans ses propres faiblesses. Tout d'abord, les autorités de certification sont des entreprises, et elles font payer leurs services. Un particulier n'est sans doute pas prêt à payer 100 euros par an juste pour prouver son identité lorsqu'il envoie des messages électroniques. Par ailleurs, les autorités de certification elles-mêmes peuvent être abusées, et leur signature numérique n'est donc pas une garantie absolue.

En fait, d'un point de vue technique ou cryptographique, il n'y a pas de différence fondamentale entre la signature numérique fournie par l'autorité de certification et les signatures que vous créez avec votre clé privée. Ce qui différencie essentiellement ces deux systèmes, c'est qu'OpenPGP vous permet de créer vous-même vos signatures numériques.

> **RAPPEL OpenPGP et certificats X.509**
>
> Le fonctionnement interne des certificats X.509 utilisés par les sites web diffère de celui de la paire de clés d'OpenPGP. Les deux ne sont pas interchangeables parce qu'ils font appel à des algorithmes différents et que leur contenu est lui aussi différent, mais les principes sont les mêmes (voir l'encadré page précédente).

Le réseau de confiance

Le réseau de confiance est le réseau infaillible des personnes qui se sont identifiées mutuellement et qui se sont signé numériquement leurs clés OpenPGP. Il est entièrement composé de liens entre individus. Avec le temps, toujours plus de personnes s'y joignent et celui-ci devient à mesure plus étendu et plus interconnecté.

ILLUSTRATION Transitivité de la confiance numérique

Supposons par exemple que je reçoive un jour un message signé numériquement par Thomas. Je n'ai jamais rencontré Thomas, mais je peux obtenir une copie de sa clé publique depuis un serveur de clés. Cette clé a été signée numériquement par des personnes qui ont vérifié son identité.

L'une des personnes ayant signé cette clé est Caroline, que je connais. Or, Caroline n'aurait pas signé la clé de Thomas sans le connaître personnellement ou sans avoir vérifié son identité d'une manière ou d'une autre. Une fois que j'ai vérifié que Caroline a signé la clé de Thomas, je sais qu'elle se « porte garante » de l'identité de Thomas. Je fais confiance à Caroline, qui fait confiance à Thomas. Il est donc très probable que la clé publique de Thomas corresponde bien à la personne Thomas.

Et la chaîne peut se poursuivre de cette manière : moi faisant confiance à Caroline, qui fait confiance à Thomas, qui fait confiance à Igor, qui fait confiance à Sarifa, et ainsi de suite.

Au fur et à mesure que la clé de Thomas est signée par un plus grand nombre de personnes, elle est de plus en plus intégrée au réseau de confiance et le nombre moyen d'intermédiaires nécessaires avant d'arriver à sa clé diminue.

Toute personne utilisant OpenPGP pour communiquer avec des tiers est connecté au réseau de confiance.

Le réseau de confiance n'est toutefois pas infaillible. Si je me fie à Caroline lorsqu'elle signe une clé parce que je sais qu'elle vérifie bien l'identité de la personne correspondante, je ne sais rien de Thomas. Peut-être signe-t-il les clés de toutes les personnes qu'il rencontre, ou bien signe-t-il des clés qu'il télécharge au hasard depuis un serveur de clés. Si OpenPGP recommençait à zéro aujourd'hui, le réseau de confiance n'aurait pas du tout le même aspect. Rappelez-vous simplement qu'en définitive, c'est toujours à vous de décider à qui vous fier. Vous pouvez toujours refuser de signer une clé ou d'accepter une identité du fait d'une relation trop distante avec la personne concernée.

Questions de confiance

De même que le mot sécurité, le mot confiance peut avoir un sens très différent selon le contexte et la personne qui l'emploie. Du reste, la norme OpenPGP évite soigneusement de le définir.

L'appartenance au réseau de confiance n'est pas un gage de bonne foi

Le fait qu'une personne fasse partie du réseau de confiance ne signifie pas qu'elle soit fiable. Vous connaissez certainement des personnes à qui vous ne confieriez ni votre portefeuille, ni votre hamster, mais vous pouvez à tout moment signer leurs clés PGP et les aider à prouver leur identité à d'autres. Ou vous pouvez très bien recevoir un message électronique signé numériquement qui soit néanmoins suspect, vous proposant par exemple d'acheter la Tour Eiffel pour quelques euros. Si la clé de l'expéditeur fait partie du réseau de confiance, vous aurez au moins quelques chances de l'identifier.

Le nombre de signatures d'une clé n'est pas une mesure de confiance

Rappel Le réseau de confiance, une responsabilité pour l'utilisateur d'OpenPGP

La responsabilité de la constitution du réseau de confiance vous incombe. L'ajout de signatures numériques d'autres utilisateurs à votre clé et la signature de clés de tiers sont des éléments importants de l'utilisation d'OpenPGP. Vous devez vous intégrer aussi bien que possible au réseau de confiance.

Le nombre de signatures ajoutées à votre clé n'est pas nécessairement une bonne indication du degré de confiance qu'on accorde à votre clé. Néanmoins, plus les chemins entre vous et un autre utilisateur du réseau de confiance sont longs et peu nombreux, moins cet autre utilisateur se fiera à votre identité. Voir « Parcourir le réseau de confiance (pathfinder) », page 159.

Signer une clé, un engagement

Lorsque vous signez la clé de quelqu'un, vous déclarez publiquement avoir identifié cette personne et avoir constaté que son identité correspond bien à celle de sa clé publique. Réciproquement, pour faire signer votre clé par un tiers, vous devez au préalable lui prouver votre identité. Nombreux sont ceux pour qui une pièce d'identité officielle comme une carte d'identité ou un passeport est une preuve d'identité suffisante.

RAPPEL Réseau de confiance vs Autorité de certification

Ce système peut sembler faillible, mais il ne l'est pas plus que celui reposant sur une autorité de certification centralisée, au sein de laquelle la certification est basée sur le travail d'êtres humains tout comme vous. Les personnes qui vérifient les identités sont formées pour détecter les faux papiers, mais elles travaillent à distance. Lorsqu'une personne vous fait face avec sa carte d'identité, vous pouvez comparer directement sa photo avec son visage, une possibilité dont l'autorité de certification ne dispose pas.

De plus, dans la mesure où nous ne vérifions pas très souvent des identités, nous sommes sans doute plus attentifs lorsque nous effectuons cette opération. Les salariés des autorités de certification ne font rien d'autre à longueur de journée. Par conséquent, le risque d'erreur humaine n'est pas négligeable, sans parler de la possibilité d'utiliser des faux papiers, qui tromperont un salarié d'une autorité de certification presque aussi facilement que vous.

Les pièces d'identité officielles ne garantissent pas l'identité d'une personne de manière sûre. Par exemple, vous hésiteriez sûrement à signer la clé d'une personne qui ne disposerait que d'un passeport tasmanien pour prouver son identité (d'autant que la Tasmanie est un état de l'Australie qui n'émet pas ses propres passeports). Vous avez parfaitement le droit de ne signer que les clés des personnes que vous connaissez bien ; c'est d'ailleurs le principe adopté par beaucoup d'utilisateurs expérimentés d'OpenPGP. Et inversement, ne soyez pas vexé si quelqu'un refuse de signer votre clé.

Intégrer le réseau de confiance

L'un des moyens les plus courants de développer vos liens dans le réseau de confiance est de participer à des séances de signature de clés (*keysigning party*). Ces réunions permettent à des utilisateurs d'OpenPGP de vérifier mutuellement leurs identités et de signer les clés les uns des autres. De telles séances sont généralement organisées en marge de conférences ou de salons spécialisés.

Si vous n'avez jamais entendu parler de la moindre séance de signature de clés ou que vous n'avez pas envie de vous y rendre, renseignez-vous autour de vous. Dès lors qu'il y a dans votre entourage des personnes en rapport avec l'informatique, vous en trouverez à coup sûr qui disposent d'une paire de clés OpenPGP.

Par ailleurs, il existe des sites spécialement conçus pour permettre aux utilisateurs d'OpenPGP de se rencontrer et d'échanger des signatures de clés, notamment www.biglumber.com.

Quoiqu'une simple signature suffit pour vous rattacher au réseau de confiance. Une fois que vous commencerez à utiliser OpenPGP, vous serez surpris de constater le nombre de personnes dans votre entourage qui l'utilisent aussi.

Précautions pour installer OpenPGP

Précautions matérielles : sur quel ordinateur installer son logiciel et ses clés ?

OpenPGP vous permet de prouver qui vous êtes. De même que vous ne laisseriez pas traîner votre carte d'identité dans un lieu public, mieux vaut éviter d'utiliser OpenPGP sur un ordinateur qui ne soit pas le vôtre. D'autres utilisateurs du même ordinateur pourraient accéder à votre trousseau de clés, et même à votre phrase secrète. Même si vous avez défini les autorisations de vos clés de telle manière que vous seul puissiez les voir, n'oubliez pas que les personnes disposant de droits d'administration pour le système pourront malgré tout accéder à ces fichiers. En d'autres termes, n'installez pas OpenPGP sur un système partagé tel que l'ordinateur de votre université ou d'un cybercafé.

Veillez également à bien protéger votre ordinateur personnel. Si vous quittez votre poste de travail sans protéger l'économiseur d'écran par un mot de passe, des personnes malintentionnées pourraient accéder à vos clés.

Précautions en cas de partage sous Windows

Parlons maintenant de Windows. Toutes les versions de Windows basées sur Windows 95 (c'est-à-dire Windows 95, 98 et Me) ne sont pas de vrais systèmes d'exploitation multi-utilisateurs. Leurs fonctions multi-utilisateurs ont été ajoutées après coup et ne sont pas véritablement intégrées au système. Par conséquent, il n'est pas possible de protéger de manière adéquate des clés OpenPGP sur un système Windows 9x. Toute personne utilisant ce système pourrait accéder à vos

clés sans que vous ne vous en rendiez jamais compte. Les fonctions de mot de passe de ces versions de Windows peuvent facilement être outrepassées par toute personne capable d'accéder au système, sans même recourir à des outils ou des logiciels spéciaux. En conséquence, nous déconseillons de stocker quelque information personnelle que ce soit, et notamment des clés OpenPGP, sur des systèmes Windows 9x.

Les systèmes d'exploitation basés sur Windows NT (Windows Vista, XP et 2000) représentent une nette amélioration dans ce domaine. Il est possible d'y accéder « par effraction », mais il faut pour cela disposer de logiciels spéciaux et de temps, comme c'est le cas pour tout bon système Unix. Toutefois, ils utilisent des comptes d'administrateur pouvant installer n'importe quoi, à la manière des comptes « root » d'Unix. Vous devez donc veiller à ce que personne d'autre ne puisse accéder à votre trousseau de clés.

Nous reviendrons sur ce sujet, mais nous ne pourrons le traiter de manière approfondie. Si vous vous intéressez à la sécurité des ordinateurs personnels, vous trouverez de nombreux livres qui traitent spécifiquement de ce sujet.

Conseils pour créer sa première paire de clés

Quelle que soit la version d'OpenPGP que vous choisissez d'utiliser, vous devez créer une paire de clés lorsque vous installez le logiciel. Les étapes à suivre diffèrent selon le logiciel, mais les principes restent les mêmes.

À RETENIR Veillez sur vos clés

Veillez à ne générer vos clés que sur une machine qui vous appartienne. Si vous laissez traîner votre paire de clés GnuPG n'importe où, n'importe qui pourrait usurper votre identité.

Choisir la longueur de la clé

La longueur de la clé est le nombre de bits (uns et zéros) dont elle est constituée. À l'heure où ces lignes sont écrites, PGP et GnuPG utilisent tous deux une valeur par défaut de 2 048 bits. Une clé symétrique de 2 048 bits suffit à assurer une sécurité forte pour les années à venir, sauf si votre attaquant dispose d'ordinateurs quantiques ou de l'un de ces ordinateurs ultrasecrets que les services de renseignements américains auraient mis en place pour casser les codes.

Vous verrez dans le prochain chapitre comment procéder avec PGP et dans le chapitre 4 comment faire avec GnuPG.

En augmentant la taille de la clé, vous augmentez la quantité de travail nécessaire pour chiffrer, mais aussi pour déchiffrer vos messages. En

contrepartie, vos clés seront plus difficiles à casser. Utilisez les paramètres par défaut, sauf si vous êtes certain que toutes les personnes avec lesquelles vous échangez des messages chiffrés disposent d'ordinateurs suffisamment puissants pour leur éviter d'avoir à faire une pause café en attendant le déchiffrement de vos messages.

Choisir le délai d'expiration des clés

La question du délai d'expiration des clés fait débat au sein même de la communauté des spécialistes d'OpenPGP. Un délai d'expiration relativement court présente certains avantages pour l'avenir : si par exemple vous laissez une paire de clés sans date d'expiration sur un CD-Rom et que quelqu'un trouve ce CD-Rom en 2038, il pourra utiliser cette paire de clés pour usurper votre identité. Avec des clés qui expirent régulièrement (au bout de quelques années), vous êtes obligé de générer à chaque fois de nouvelles clés et de les diffuser ensuite auprès de vos correspondants.

En tant que nouvel utilisateur d'OpenPGP, vous constaterez sans doute assez vite que certains choix que vous avez faits lors de la création des clés n'étaient pas les meilleurs. Il est alors plus difficile de se débarrasser d'une clé qui n'expire jamais. Pour votre première clé, nous conseillons un délai d'expiration d'un an. Pour vos clés suivantes, choisissez des délais d'expiration allant de deux à cinq ans. Bien que dans ce livre, nous fassions de notre mieux pour aborder et résoudre tous les problèmes potentiels auxquels vous pourriez être confronté, vous trouverez sans doute des manières d'utiliser OpenPGP que nous n'aurions jamais imaginées, d'où l'intérêt de choisir des délais d'expiration relativement courts.

Le problème le plus courant des clés qui n'expirent pas est sans doute la situation où une vieille clé publique est employée pour contacter quelqu'un qui ne dispose plus de la paire de clés, et par conséquent, ne peut pas lire les messages qui lui sont adressés. Si vous aviez par exemple rendu publique une clé PGP sans date d'expiration en 1995, elle serait encore disponible aujourd'hui par l'intermédiaire de Google et d'autres sites web ; vous auriez du mal à retrouver les logiciels nécessaires pour lire un message chiffré avec cette clé. Il vous serait encore plus difficile de lire un tel message en 2015, mais la clé serait encore en cache à divers endroits, et quels que soient vos efforts pour diffuser une clé mise à jour, toutes sortes de personnes continueraient à utiliser l'ancienne.

Retenez qu'il faut toujours choisir un délai d'expiration pour vos clés.

Nom, adresse électronique et commentaire

Votre nom, votre adresse électronique et un commentaire facultatif se combinent pour créer votre identifiant utilisateur OpenPGP, ou UID (*User ID*). Veillez à ne pas faire d'erreur lors de la saisie de ces informations.

Nom

Utilisez vos vrais nom et prénom. Rappelez-vous que l'un des aspects essentiels de l'utilisation de GnuPG est de faire signer votre clé publique par des tiers. S'il est facile de faire signer sa clé à ses amis et parents, il est plus difficile de prouver son identité à des étrangers.

Pour prouver votre identité à quelqu'un que vous rencontrez pour la première fois de votre vie, mieux vaut que le nom de la clé corresponde aussi exactement que possible à celui d'une pièce identité officielle.

Adresse électronique

Vous devez également indiquer une adresse électronique. Votre clé est liée à cette adresse électronique, pour le meilleur et pour le pire.

Notez que vous pouvez bien sûr associer autant d'adresses électroniques que souhaité à une clé.

Commentaire

Le commentaire sert généralement à décrire en quelques mots qui vous êtes et ce que vous faites. Il peut être important dans la mesure où il arrive que deux personnes aient les mêmes nom et prénom. Ainsi, une recherche Google portant sur « Michael Lucas » vous permettra de trouver toute une série de personnages intéressants : doubleurs, acteurs, professeurs de tir, ministres, etc.

Identifiant utilisateur

La combinaison de ces trois informations, nom, adresse électronique et commentaire, est l'identifiant utilisateur ou UID. Un UID est censé se référer à une seule entité. Lorsque quelqu'un cherche votre clé privée, il doit pouvoir la trouver en se basant sur votre nom, ou à défaut sur votre adresse électronique.

Une personne qui cherche à vous contacter n'essaiera probablement pas de trouver votre clé publique en effectuant une recherche sur votre activité. Toutefois, cette mention, dans les commentaires, lui permettra de vous distinguer de tous vos homonymes qui utilisent OpenPGP.

Créer un certificat de révocation dès la création de la clé

Un certificat de révocation vous permet d'annoncer au monde que votre paire de clés n'est plus valide. Vous en aurez besoin si vous perdez votre clé privée ou si quelqu'un s'en empare. De même, si vous oubliiez votre phrase secrète, vous ne pourrez plus utiliser votre propre clé privée ni lire les messages électroniques chiffrés que vous recevez.

Il n'est pas impossible non plus que les évolutions technologiques rendent obsolète votre paire de clés. Vous entendrez parler de temps à autre d'un utilisateur recevant un message chiffré avec une clé PGP datant de 1992 dans un format qu'aucun logiciel OpenPGP moderne ne peut lire. C'est peut-être la raison la plus importante pour laquelle il est préférable de choisir une date d'expiration pour votre clé.

Dans ces situations, vous avez besoin d'un moyen de « désactiver » votre clé. Aussi conseillons-nous pour parer à ces éventualités de créer le certificat de révocation immédiatement après avoir créé la clé.

Stocker en lieu sûr sa paire de clés

Après avoir commencé à utiliser OpenPGP, la perte de votre clé privée vous causerait des problèmes interminables. Des fichiers ont disparu à la suite d'erreurs des utilisateurs, il est arrivé que des bogues de système de fichiers effacent des données dont l'importance est apparue des semaines plus tard, et des bogues de système d'exploitation peuvent empêcher tout démarrage d'une machine. Trois des ordinateurs de l'auteur ont pris feu. Alors que dans le monde de l'entreprise, on peut toujours accuser le département informatique en cas de problème, vous êtes le seul à pouvoir protéger vos clés OpenPGP. Vous ne pouvez déléguer cette responsabilité.

ATTENTION
Évitez les ordinateurs publics

Ne stockez ni votre paire de clés, ni votre certificat de révocation sur un ordinateur public, semi-public ou utilisé par plusieurs personnes à la fois.

Effectuez une copie de sauvegarde de votre paire de clés et de votre certificat de révocation sur un support amovible, CD-Rom, par exemple, et stockez-le en lieu sûr, par exemple dans le coffre-fort d'une banque. Vous pourriez également les emmener avec vous sur une clé USB ou un lecteur MP3 à condition de les chiffrer au préalable.

Le coffre-fort est une solution relativement sûre. Cependant, si un coffre-fort résistant au feu évite la combustion de son contenu en cas d'incendie, les températures atteintes suffisent pour corrompre les supports numériques. Vous pouvez par conséquent imprimer votre certificat

de révocation et le stocker en même temps que sa sauvegarde numérique. Ainsi, en cas de défaillance du support, vous aurez la possibilité de copier manuellement le certificat pour révoquer votre clé.

Stocker un certificat de révocation

De même que toute personne mettant la main sur votre clé privée et votre phrase cachée peut se faire passer pour vous, toute personne obtenant votre certificat de révocation pourrait rendre votre clé publique inutilisable. Ce serait ennuyeux pour un débutant et catastrophique pour un utilisateur faisant fréquemment appel à OpenPGP. Stockez votre certificat de révocation aussi sûrement que votre clé privée.

Identification photographique et clés OpenPGP

Depuis peu, il est possible de stocker une image dans une clé publique OpenPGP. La vérification de l'identité du propriétaire de la clé est ainsi beaucoup plus facile, puisqu'une image est visible au moment de signer ou non sa clé. PGP et GnuPG permettent tous deux d'extraire et d'afficher les photos incluses dans les clés.

Taille et format de la photo

Pour insérer votre propre photo dans votre clé, vous devez disposer d'une image numérique de vous-même qui montre soit votre visage seul, soit votre tête et vos épaules. Pour le meilleur résultat possible, l'image doit mesurer 120×144 pixels et être au format JPEG. Ces paramètres sont valables à la fois pour PGP et GnuPG. Les clés OpenPGP doivent être aussi compactes que possible ; par conséquent, veillez à ce que votre photo soit la moins volumineuse possible. Elle n'a pas besoin d'être très détaillée : il suffit que vous soyez reconnaissable.

> L'insertion d'une photo dans votre clé publique n'est pas difficile, mais nécessite des connaissances dont vous ne disposez pas encore. Nous y reviendrons aux chapitres 6 (pour PGP) et 7 (pour GnuPG).

Diffuser sa clé publique

PRÉCAUTION Petite vérification avant la publication de la clé

Avant de faire profiter le monde entier de votre clé publique, assurez-vous que vous êtes prêt à utiliser OpenPGP. Effectuez une sauvegarde de vos clés publique et privée. Créez un certificat de révocation. Stockez le tout en lieu sûr. Si vous n'effectuez pas ces opérations, vous risquez de poster une clé « orpheline », ce qui veut dire que vous recevrez des messages chiffrés (et potentiellement importants) sans pouvoir les déchiffrer. En cas de doute, patientez un peu avant de poster votre clé sur un serveur de clés. Il sera toujours temps de le faire un peu plus tard.

Vous vous dites peut-être que la meilleure chose à faire est de proposer votre clé publique en téléchargement sur votre page web, mais en réalité, ce n'est pas nécessairement une bonne idée. N'importe qui peut créer une page web indiquant « Site officiel de Michael W. Lucas » et y placer une clé publique. Pire encore : n'importe qui pourrait indiquer sur cette page web « Pour contacter l'auteur mondialement connu de *PGP et GPG* et d'autres ouvrages informatiques érudits, envoyez-lui un message à l'adresse michaellucasauteurinformatique@hotmail.com et utilisez cette clé OpenPGP ». Bien entendu, l'adresse qui précède n'est pas la véritable adresse électronique de l'auteur.

Vous verrez parfois des signatures de messages électroniques indiquant « Ma clé publique est disponible à l'adresse www.monsiteweb.com ». Cette approche semble meilleure, à en juger par le grand nombre de personnes qui l'utilisent. Toutefois, le message électronique aurait pu être altéré, et l'URL pourrait donc avoir été falsifiée afin de tromper le destinataire. En revanche, si l'expéditeur envoie beaucoup de messages électroniques, ses correspondants peuvent s'assurer que l'URL indiquée est bien la même dans tous les messages.

Le meilleur moyen de distribuer une clé est de la fournir en personne. Lorsqu'un collègue crée une paire de clés OpenPGP, demandez-lui de vous envoyer sa clé publique, vérifiez-la ensemble, puis ajoutez-la à votre trousseau de clés.

À l'évidence, cette solution ne peut être employée pour tous vos correspondants, partout dans le monde. Par ailleurs, il n'est pas possible non plus de demander par courrier électronique la clé publique d'un message

chiffré que vous venez de recevoir : vous n'auriez aucune garantie quant à l'identité de l'expéditeur.

Heureusement, OpenPGP dispose d'un mécanisme de distribution de clés que nous avons déjà évoqué, et qui couvre le monde entier.

Recourir à des serveurs publics de clés

Il existe des serveurs Internet spécifiquement conçus pour gérer et distribuer des clés OpenPGP. Ces serveurs de clés sont semblables aux autres serveurs Internet qui sont configurés pour traiter les pages web, le courrier électronique ou tout autre protocole.

Les logiciels OpenPGP sont capables de communiquer automatiquement avec des serveurs de clés OpenPGP.

Les serveurs de clés sont très nombreux et distribués dans le monde entier. Ils s'échangent généralement leurs bases de données entre eux pour que toutes les clés soient accessibles sur tous les serveurs.

Les serveurs de clés OpenPGP traditionnels permettaient à n'importe qui d'ajouter une clé avec n'importe quelle adresse électronique. Aujourd'hui, avec l'explosion du nombre d'utilisateurs d'Internet, cette approche laisse apparaître ses limites. La société PGP Corporation propose un service de « clé PGP vérifiée ». Lorsque vous envoyez une clé, vous recevez un message électronique à l'adresse de la clé pour confirmer celle-ci. C'est une sécurité supplémentaire, qui nécessite que Mallory puisse accéder au compte de courrier électronique de la personne dont elle cherche à usurper l'identité. Dans ce cas toutefois, OpenPGP ne représentera pas un obstacle pour elle.

Limites du système de diffusion par serveurs

Les réserves exprimées quant à la fiabilité et à l'intégrité du système de serveurs de clés sont en partie légitimes. Il a été conçu et mis en place avant qu'Internet ne se popularise, et il faut maintenant vivre avec ses limitations. Si le système OpenPGP était recréé à partir de zéro aujourd'hui, les solutions trouvées seraient sans doute différentes, mais on peut dire la même chose du Web, du courrier électronique et de tous les autres protocoles qui font d'Internet ce qu'il est aujourd'hui. Il faut aussi se rappeler que le système de serveurs de clés est de loin supérieur au système de vérification d'identité par défaut d'Internet, qui est inexistant.

Publier sa clé publique sur son site web

Les serveurs de clés ne sont pas la seule solution pour distribuer votre clé publique. Rien ne vous empêche de la proposer en téléchargement sur votre site web : elle confirmera un peu plus que vous êtes bien qui vous prétendez être, pour tous ceux qui sont suffisamment paranoïaques pour effectuer ce type de vérification sur votre site.

Beaucoup d'utilisateurs de systèmes de type Unix partagés placent leur clé publique dans leur fichier `finger text` ou `plan` pour le rendre accessible aux autres utilisateurs du système. Si ces méthodes sont parfaitement légitimes en tant que moyens de diffusion supplémentaires, elles ne s'intègrent pas bien à l'architecture d'OpenPGP. L'utilisateur moyen d'OpenPGP n'aura pas nécessairement envie d'essayer de retrouver la page web de son correspondant : il voudra que son logiciel de courrier électronique se procure automatiquement la clé sur un serveur de clés.

Diffusion ad hoc

Certaines personnes ont des raisons particulières de ne pas vouloir utiliser des serveurs de clés, par exemple parce qu'elles ne souhaitent pas que des inconnus leur envoient des messages chiffrés, ou encore parce qu'elles ont des objections de principe quant à la sécurité de l'architecture des serveurs de clés. Ces personnes utilisent leurs propres méthodes pour diffuser leurs clés, et vous devrez respecter la procédure qu'elles imposent si vous souhaitez leur envoyer des messages chiffrés.

Maintenant que vous savez à quoi va vous servir le logiciel que vous avez choisi, il est temps de s'intéresser à l'installation de PGP et de GnuPG.

À RETENIR **Résumons !**

- On chiffre donc avec les clés publiques (souvent publiquement disponibles de ses destinataires).
- On signe avec sa propre clé privée — les destinataires vérifiant la signature grâce à la clé publique correspondante.

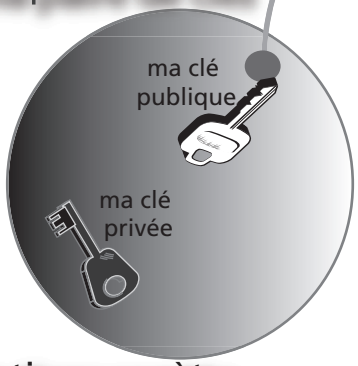
On peut chiffrer avec autant de clés que souhaité (pour autant de destinataires) et il est recommandé de toujours chiffrer aussi avec sa propre clé publique afin d'être en mesure plus tard de déchiffrer ses propres messages.

OpenPGP

Je publie ma clé publique.

Mes correspondants l'utilisent pour m'adresser des messages chiffrés.

Je sauvegarde ma paire de clés



Je tiens secrète ma clé privée.

Pour déchiffrer un message qui m'est destiné, j'utilise ma clé privée.

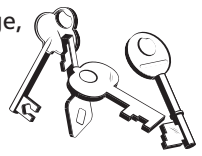
Pour chiffrer un message, j'utilise les clés publiques de mes correspondants.

Pour pouvoir relire un message que j'ai chiffré pour d'autres, je le chiffre aussi avec ma clé publique.

Pour vérifier la signature de mon correspondant, j'utilise sa clé publique.

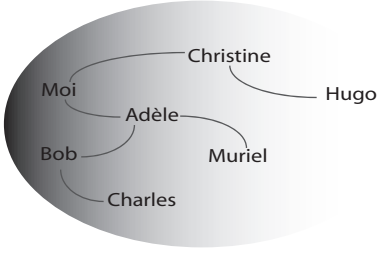
Pour signer un message j'utilise ma clé privée. Mon correspondant vérifie ma signature avec ma clé publique.

Pour chiffrer et signer un message, je le chiffre avec la clé publique de mon correspondant, je le signe avec ma clé privée.



mon trousseau de clés

Les clés publiques de mes correspondants me sont remises directement ou bien je les trouve sur un serveur de clés. Je m'en sers après avoir vérifié leur empreinte.



le réseau de confiance

Lorsque je me suis assuré (de visu) de l'identité du propriétaire d'une clé, je peux signer sa clé et étendre le réseau de confiance. J'ai d'autant plus confiance en une clé qu'elle est signée de moi ou de gens en qui j'ai confiance.