Gestion des clés PGP

La gestion des clés PGP est le processus de création, de distribution et de sécurisation des clés cryptographiques utilisées pour le chiffrement et les signatures numériques.

Il s'agit d'un processus essentiel pour la protection des communications chiffrées et la vérification de l'authenticité de l'expéditeur.

La gestion des clés repose sur une paire de clés publique/privée:

Clé publique [#public] :

Partagée publiquement. Toute personne peut utiliser votre clé publique pour chiffrer un message à votre place ou vérifier votre signature numérique.

Clé privée [#private] :

Conservée secrète et protégée par une phrase de passe robuste. Vous l'utilisez pour déchiffrer les messages qui vous sont envoyés et pour créer des signatures numériques.

Nous abordons ci-dessous quatre aspects fondamentaux de la gestion des clés PGP.

1. Génération de clés

Créer des paires de clés:

Utilisez un logiciel comme GnuPG (GPG) pour générer une paire de clés publique/privée.

Établir une clé principale et des sous-clés : Créez une clé principale pour les certifications, puis utilisez des sous-clés pour les opérations courantes, comme la signature et le chiffrement.

La clé principale doit être stockée hors ligne, tandis que les sous-clés peuvent être stockées sur vos appareils.

Utiliser des phrases de passe robustes:

Protégez votre clé privée avec une phrase de passe complexe et unique. La sécurité de PGP dépend de la robustesse de sa phrase de passe.

Définir une date d’expiration:

Il est recommandé de définir une date d’expiration pour vos clés (par exemple, dans un délai de deux ans).

Cela vous oblige à générer une nouvelle clé à intervalles régulières, rendant ainsi obsolètes les clés anciennes, compromises ou oubliées.

Générer un certificat de révocation:

Immédiatement après la création d’une nouvelle clé, générez un certificat de révocation.

Conservez ce certificat en lieu sûr, séparément de votre clé privée.

En cas de perte ou de compromission de votre clé privée, ce certificat vous permet de la révoquer publiquement.

2. Distribution et vérification des clés

Partagez votre clé publique:

Distribuez votre clé publique aux personnes qui doivent vous envoyer des messages chiffrés ou vérifier votre signature.

Vous pouvez le faire en la téléchargeant sur un serveur de clés publiques ou en la partageant sous forme de fichier ASCII chiffré (.asc).

Importez des clés publiques:

Lorsque vous souhaitez envoyer un message chiffré à quelqu'un, vous devez d'abord importer sa clé publique dans votre trousseau de clés.

Vérifiez l'authenticité de la clé:

Vous ne devez jamais faire aveuglément confiance à une clé publique provenant d'un serveur de clés.

Vous devez plutôt vérifier l'authenticité d'une clé en comparant son empreinte numérique via un canal de confiance (par exemple, par téléphone ou en personne).

Utilisation du réseau de confiance:

Le modèle original de PGP utilise un "réseau de confiance" pour garantir l'authenticité des clés.

Les utilisateurs peuvent signer cryptographiquement la clé d'un autre utilisateur pour certifier avoir vérifié que cette clé lui appartient.

Votre logiciel peut ensuite utiliser ces signatures tierces pour déterminer le niveau de confiance qu'il accorde à une clé.

3. Maintenance continue

Sécurisez votre clé privée:

Votre clé privée est votre actif le plus précieux.

Stockez-la sur un ordinateur doté de contrôles d'accès robustes, ou sur un périphérique chiffré et hors ligne, comme une clé USB.

Sauvegardez vos clés:

Sauvegardez régulièrement vos trousseaux de clés publique et privée.

C'est crucial, car si vous perdez votre clé privée ou oubliez votre phrase secrète, vous ne pourrez déchiffrer aucun message (ancien ou actuel).

Changez vos phrases secrètes:

Changez régulièrement votre phrase secrète, surtout si vous soupçonnez qu'elle a été compromise.

Révoquer les clés compromises ou expirées:

Si une clé privée est compromise ou arrive à expiration, vous devez la révoquer immédiatement et en émettre une nouvelle.

Le certificat de révocation que vous avez généré précédemment vous permet d'effectuer cette opération.

4. Outils de gestion des clés PGP

Conseils pratiques:

Conseils pratiques sur les clés GPG tirés de l'article d'Alex Cabal (anglais)

Gnu Privacy Guard (GnuPG ou GPG) :

Un outil en ligne de commande gratuit et open source, qui implémente intégralement la norme OpenPGP. C'est l'outil le plus courant pour la gestion manuelle des clés PGP et il s'intègre à de nombreuses applications.

Gpg4win:

Une version Windows de GnuPG incluant des outils graphiques pour la gestion des clés et l'intégration avec des applications telles que Microsoft Outlook.

Kleopatra:

Un gestionnaire de certificats inclus dans Gpg4win offrant une interface utilisateur graphique pour la gestion des clés.

Plateformes gérées:

Pour les environnements d'entreprise, des outils comme IBM Sterling B2B

Integrator et Symantec Encryption Management Server offrent des fonctionnalités de gestion automatisée des clés, telles que le stockage sécurisé et le contrôle côté serveur de l'expiration des clés.

Fournisseurs de messagerie web:

Des services comme Proton Mail intègrent la gestion des clés PGP de manière transparente, gérant la création, le chiffrement et le déchiffrement en arrière-plan.

---

1 **Confiance**:

Lorsque nous parlons de confiance envers les clés publiques, nous nous inquiétons de la possibilité qu’une personne autre que le destinataire prévu d’un message chiffré, ayant publié une clé frauduleuse, vous trompe en vous incitant à chiffrer un message que sa propre clé, et non celle du véritable destinataire, peut déchiffrer.

Nous craignons également qu’une personne mal intentionnée vous envoie des messages signés numériquement comme s’ils provenaient de l’expéditeur légitime.

Pour atténuer ces risques, nous devons être extrêmement vigilants quant à l’endroit et la manière dont nos clés publiques sont partagées et vérifiées.

2 **Clé publique**:

Il incombe à votre infrastructure de sécurité de protéger l'emplacement où les clés publiques sont mises à disposition contre tout accès en écriture non autorisé.

Bien que les clés publiques ne soient pas conservées privées, elles doivent néanmoins être authentiques.

C'est pourquoi les serveurs de clés publiques doivent vérifier les insertions en exigeant des codes d'authentification lors des transactions d'insertion.

3 **Clé privée**:

Protégez le fichier de clé privée avec une phrase de passe robuste et n'autorisez á aucun sinon le propriétaire y accéder en lecture.

Quiconque a accès à une clé privée peut l'utiliser pour créer des signatures numériques et déchiffrer des messages secrets.

Il est primordial de ne jamais partager ces clés avec qui que ce soit; la phrase de passe qui les protège doit être robuste.

Le fichier de clé chiffré par la phrase de passe doit également être inaccessible à toute personne autre que le propriétaire, rendant ainsi les techniques de force brute pour casser la phrase de passe impraticables.