Gestión de claves PGP

La gestión de claves PGP es el proceso de crear, distribuir y proteger las claves criptográficas utilizadas para el cifrado y las firmas digitales.

Este es un proceso fundamental para salvaguardar las comunicaciones cifradas y verificar la autenticidad del remitente.

La gestión de claves se basa en un par de claves pública-privada:

Clave pública [2]:

Se comparte abiertamente con otros. Cualquiera puede usar tu clave pública para cifrar un mensaje o verificar tu firma digital.

Clave privada [3]:

Se mantiene en secreto y está protegida por una contraseña segura. Se utiliza para descifrar los mensajes que recibes y para crear firmas digitales.

A continuación, analizamos cuatro áreas clave de la gestión de claves PGP.

1. Generación de claves

Crear pares de claves:

Utilice software como GnuPG (GPG) para generar un par de claves pública-privada.

Establecer una clave maestra y subclaves: Cree una clave maestra para las certificaciones y utilice las subclaves para las operaciones diarias, como la firma y el cifrado.

La clave maestra debe almacenarse sin conexión, mientras que las subclaves pueden almacenarse en sus dispositivos.

Utilizar contraseñas seguras:

Proteja su clave privada con una contraseña compleja y única. La seguridad de PGP depende de la seguridad de la contraseña.

Establecer una fecha de caducidad:

Es recomendable establecer una fecha de caducidad para sus claves (por ejemplo, en un plazo de dos años). Esto le obliga a generar una nueva clave periódicamente, lo que hace que las claves antiguas, comprometidas u olvidadas queden obsoletas con el tiempo.

Generar un certificado de revocación:

Inmediatamente después de crear una nueva clave, genere un certificado de revocación.

Guarde este certificado en un lugar seguro, separado de su clave privada. En caso de que su clave privada se pierda o sea comprometida, este certificado le permitirá revocar públicamente la clave.

2. Distribución y verificación de claves

Comparte tu clave pública:

Distribuye tu clave pública a quienes necesiten enviarte mensajes cifrados o verificar tu firma.

Esto se puede hacer subiéndola a un servidor de claves públicas o compartiéndola como un archivo ASCII (.asc).

Importar claves públicas:

Cuando quieras enviar un mensaje cifrado a otra persona, primero debes importar su clave pública a tu llavero.

Verificar la autenticidad de la clave:

Nunca debes confiar ciegamente en una clave pública de un servidor de claves.

Debes verificar la autenticidad de una clave comparando su huella digital a través de un canal de confianza (por ejemplo, mediante una llamada telefónica o en persona).

Utilice la Red de Confianza:

El modelo original de PGP utiliza una "red de confianza" para verificar la autenticidad de las claves.

Los usuarios pueden firmar criptográficamente la clave de otro usuario para certificar que han verificado que pertenece a esa persona.

Su software puede utilizar estas firmas de terceros para determinar el grado de confianza que deposita en una clave.

3. Mantenimiento continuo

Proteja su clave privada:

Su clave privada es su activo más valioso.

Guárdela en un equipo con controles de acceso robustos o en un dispositivo cifrado y sin conexión, como una memoria USB.

Realice copias de seguridad de sus claves:

Realice copias de seguridad periódicas de sus llaveros de claves pública y privada. Esto es crucial, ya que si pierde su clave privada u olvida su contraseña, no podrá descifrar ningún mensaje (ni antiguos ni actuales).

Cambie su contraseña:

Cambie su contraseña periódicamente, especialmente si sospecha que puede haber sido comprometida.

Revoque las claves comprometidas o caducadas:

Si una clave privada se ve comprometida o caduca, debe revocarla inmediatamente y emitir una nueva.

El certificado de revocación que generó anteriormente lo permite.

4. Herramientas para la gestión de claves PGP

Consejos prácticos:

Consejos prácticos sobre claves GPG del artículo de Alex Cabal (ingles)

Gnu Privacy Guard (GnuPG o GPG):

Una herramienta de línea de comandos gratuita y de código abierto que implementa completamente el estándar OpenPGP.

Es la herramienta más común para la gestión manual de claves PGP y se integra con numerosas aplicaciones.

Gpg4win:

Una versión de GnuPG para Windows que incluye herramientas gráficas para gestionar claves e integrarse con aplicaciones como Microsoft Outlook.

Kleopatra:

Un gestor de certificados incluido en Gpg4win que proporciona una interfaz gráfica de usuario para la gestión de claves.

Plataformas gestionadas:

Para entornos corporativos, herramientas como IBM Sterling B2B Integrator y Symantec Encryption Management Server ofrecen funciones de gestión de claves automatizadas, como almacenamiento seguro y control del servidor sobre la caducidad de las claves.

Proveedores de correo web:

Servicios como Proton Mail integran la gestión de claves PGP de forma impecable, encargándose de la creación, el cifrado y el descifrado en segundo plano.

---

1 **Confianza**:

Cuando hablamos de confiar en las claves públicas, nos preocupa la posibilidad de que alguien distinto del destinatario previsto de un mensaje cifrado, que haya publicado una clave de enmascaramiento, le engañe para que cifre un mensaje que su clave, en lugar de la del destinatario real, pueda descifrar.

También nos preocupa que un enmascarador le envíe mensajes firmados digitalmente como si provinieran del remitente legítimo.

Para mitigar estos riesgos, debemos ser meticulosos con respecto a dónde y cómo se comparten y verifican nuestras claves públicas.

2 **Clave pública**:

Es responsabilidad de su infraestructura de seguridad proteger la ubicación donde se ponen a disposición las claves públicas del acceso de escritura no autorizado. Aunque las claves públicas no se mantienen privadas, deben ser auténticas. Por eso, los servidores de claves públicas deben verificar las inserciones exigiendo códigos de autenticación durante las transacciones de inserción.

3 **Clave privada**:

Proteja el archivo de clave privada con una contraseña segura y no permita que nadie más que el propietario acceda a él. Nunca la comparta.

Cualquier persona que tenga acceso a una clave privada puede usarla para crear firmas digitales y también para descifrar mensajes secretos. Es muy importante no compartir nunca estas claves con nadie; la contraseña que las protege debe ser segura.

El archivo de clave cifrado con la contraseña también debe ser inaccesible para cualquier persona que no sea el propietario, lo que hace que las técnicas de fuerza bruta para descifrar la contraseña sean prácticamente imposibles.