LABORATORIO DE CERTIFICADOS DIGITALES ENTREGA II: FIRMA DIGITAL DE DOCUMENTOS PDF EN KALI LINUX

Jhon Edison Hincapie Garcia

Febrero 2025

Universidad Politécnico Grancolombiano
Especialización en Seguridad de la Información
Materia: Criptografía Asimétrica
Docente: José Alfonso Valencia Rodríguez

1 Introducción

En la era digital, la autenticidad y la integridad de los documentos son aspectos fundamentales para garantizar la seguridad de la información. La firma digital es una técnica criptográfica que permite validar la autenticidad de un documento y asegurar que no haya sido alterado. En este documento, se presentará un laboratorio práctico para firmar documentos PDF en Kali Linux, además de una explicación detallada sobre los certificados digitales y su validación.

2 Materiales y Requerimientos

Para realizar este laboratorio, se necesita:

- Kali Linux instalado.
- GnuPG (GPG) para la gestión de claves.
- LibreOffice para la creación de archivos PDF (opcional).
- OpenSSL para verificación de firmas digitales.

3 Procedimientos creación de firmas digitales

3.1 Paso 1:Generación de Claves GPG

Ejecutar el siguiente comando para generar un par de claves:

```
gpg --full-generate-key
```

Seleccionar el tipo de clave, el tamaño (recomendado 4096 bits) y configurar los datos de usuario.

3.2 Paso 2: Creación del Documento PDF

Para generar un PDF desde un archivo de texto:

```
echo "Este es un documento de prueba PARA COMPROBAR EL FIRMADO DIGITAL" > documento.txt
libreoffice --convert-to pdf documento.txt
```

3.3 Paso 3: Firma Digital del Documento PDF

Para firmar el documento con GPG:

```
gpg --detach-sign --armor --output documento.pdf.sig documento.pdf
```

Esto genera un archivo de firma digital ‘documento.pdf.sig‘.

3.4 Paso 4: Verificación de la Firma Sin Alterar

Para comprobar la autenticidad del documento firmado:

```
gpg --verify documento.pdf.sig documento.pdf
```

Si la firma es válida, se confirmará que el documento no ha sido alterado.

3.5 Paso 5: Simulación de Alteración del Documento

Para comprobar qué sucede si el documento es modificado después de la firma, edítalo de la siguiente manera:

```
echo "Texto alterado" >> documento.txt
libreoffice --convert-to pdf documento.txt --outdir .
```

Luego, intenta verificar la firma nuevamente:

```
gpg --verify documento.pdf.sig documento.pdf
```

Si el documento ha sido alterado, GPG mostrará un mensaje de error indicando que la firma no es válida.

3.6 Paso 6: Exportar la Clave Pública (Opcional, para Verificación en Otro Equipo)

Si deseas verificar la firma en otro equipo, es necesario exportar la clave pública y compartirla:

```
gpg --export -a "Tu Nombre" > clave_publica.asc
```

En el otro equipo, se puede importar la clave pública con:

```
gpg --import clave_publica.asc
```

Esto permitirá verificar la firma en otro dispositivo de manera segura.

4 Aplicación del Certificado Digital en el Laboratorio

4.1 Generación del Certificado Digital

Para generar un certificado digital en Kali Linux, utilizamos OpenSSL. Esto permitirá crear un certificado autofirmado para su uso en firmas digitales y validación de documentos.

4.1.1 Generar una clave privada RSA de 2048 bits:

```
openssl genpkey -algorithm RSA -out clave_privada.key -pkeyopt rsa_keygen_bits:2048
```

4.1.2 Crear una solicitud de certificado (CSR):

```
openssl req -new -key clave_privada.key -out solicitud.csr
```

Durante este paso, se solicitará información como el país, la organización y el correo del usuario.

4.1.3 Generar el certificado digital autofirmado (válido por 1 año):

```
openssl x509 -req -days 365 -in solicitud.csr -signkey clave_privada.key -out certificado.crt
```

4.1.4 Verificar que el certificado se generó correctamente:

```
openssl x509 -in certificado.crt -noout -text
```

4.2 Instalación del Certificado Digital en Kali Linux

Para que el sistema reconozca el certificado, se debe agregar a la lista de certificados de confianza:

4.2.1 Copiar el certificado a la ubicación de certificados del sistema:

```
sudo cp certificado.crt /usr/local/share/ca-certificates/
```

4.2.2 Actualizar la base de datos de certificados:

```
sudo update-ca-certificates
```

4.2.3 Verificar que el certificado fue agregado correctamente:

```
openssl verify -CAfile /etc/ssl/certs/ca-certificates.crt certificado.crt
```

4.3 Uso del Certificado Digital para Firmar un Documento

Con el certificado instalado, podemos firmar digitalmente documentos en PDF:

4.3.1 Convertir un archivo de texto a PDF:

```
echo "Este es un documento de prueba" > documento.txt
libreoffice --convert-to pdf documento.txt
```

4.3.2 Firmar digitalmente el documento con GPG:

```
gpg --detach-sign --armor --output documento.pdf.sig documento.pdf
```

Esto generará un archivo .sig que representa la firma digital del documento.

4.3.3 Verificación de la Firma Digital

```
gpg --verify documento.pdf.sig documento.pdf
```

Si la firma es auténtica y el documento no ha sido alterado, se mostrará un mensaje confirmando la validez.

4.4 Exportación e Importación de Certificados

Si es necesario compartir el certificado con otros usuarios para validación:

4.4.1 Exportar la clave pública para verificación

```
gpg --export -a "Nombre del Usuario" > clave_publica.asc
```

4.5 Importar un certificado digital de otro usuario:

```
gpg --import clave_publica.asc
```

Estos procesos garantizan la autenticidad, integridad y no repudio de los documentos electrónicos, asegurando que la información transmitida no sea alterada y que el firmante sea legítimo. La correcta aplicación de certificados digitales es clave en sistemas modernos donde la seguridad y la confianza en los documentos electrónicos son fundamentales.

5 Práctica aplicada

5.1 Video Explicativo

+ Ver Video Parte I- Firma Digital del Documento PDF
  + Ver Video Parte II - Generación del Certificado Digital

5.2 Repositorio de Código GitHub

Ver Laboratorio Paso a Paso Completo

5.3 Conclusión de la práctica aplicada

Este laboratorio nos permitió explorar el uso de herramientas en Kali Linux para aplicar firmas digitales en documentos, utilizando algoritmos como RSA, ECDSA y SHA-256. A través de cada paso, demostramos cómo garantizar la integridad, autenticidad y el no repudio en la información digital.

Sin embargo, este ejercicio nos deja una interrogante clave: ¿Las empresas realmente están aplicando estos procedimientos en sus sistemas y comunicaciones?

En un mundo donde la seguridad digital es fundamental, muchas compañías del sector tecnológico —y otras que manejan datos sensibles— deberían implementar estos mecanismos para proteger la información que envían y reciben. No solo se trata de cumplir normativas, sino de generar confianza en los usuarios y clientes.

¿Las empresas realmente garantizan el no repudio en la mayoría de los casos?

Si una organización no firma digitalmente sus documentos o comunicaciones, ¿cómo se asegura de que no sean modificados o falsificados? Si los clientes envían información sensible, ¿pueden estar seguros de que no será alterada sin su consentimiento? Este laboratorio demuestra que las herramientas para firmar y validar información digitalmente están al alcance de todos. La pregunta es: ¿Se están utilizando de manera efectiva en el mundo real?

6 Preguntas y Respuestas

6.1 ¿Qué garantiza el uso de firmar un documento?

El uso de una firma digital garantiza tres aspectos fundamentales en un documento electrónico:

- **Autenticidad:** Permite confirmar la identidad del firmante, asegurando que el documento ha sido firmado por la persona o entidad legítima.
- **Integridad:** Garantiza que el contenido del documento no ha sido alterado después de la firma. Cualquier modificación posterior será detectada y la firma será inválida.
- **No repudio:** Evita que el firmante pueda negar haber firmado el documento, ya que la firma digital está vinculada de manera única a su clave privada.

Este proceso es crucial en ámbitos como contratos electrónicos, comunicaciones empresariales y procesos legales, donde se requiere garantizar la validez y seguridad de la información.

6.2 ¿Qué función realiza el certificado digital y cómo se relaciona con la firma digital?

Un certificado digital asocia una clave pública con la identidad del usuario y es fundamental para validar la autenticidad de la firma digital.

Un certificado digital es un documento electrónico emitido por una Autoridad de Certificación (CA) que asocia una clave pública con la identidad de un usuario o entidad. Su función principal es garantizar la autenticidad del firmante y permitir la verificación de su firma digital.

La relación entre el certificado digital y la firma digital es clave:

- **Firma Digital:** Se genera mediante una clave privada y permite garantizar la integridad del documento.
- **Certificado Digital:** Contiene la clave pública correspondiente y permite a terceros verificar la validez de la firma digital.

Cuando alguien recibe un documento firmado, puede utilizar el certificado digital del firmante para validar que la firma es auténtica y que la información no ha sido alterada.

6.3 ¿Qué proceso permite validar los certificados y firmas digitales?

La validación se realiza mediante la verificación de la firma digital y la autenticidad del certificado digital utilizando la cadena de confianza.

- **Verificación de la firma digital:** Se utiliza la clave pública del firmante (proporcionada en su certificado digital) para comprobar si la firma es válida y si el contenido del documento no ha sido modificado.
- **Autenticidad del certificado digital:** Se valida el certificado digital del firmante verificando su cadena de confianza, es decir, si ha sido emitido por una Autoridad de Certificación confiable.
- **Uso de la Cadena de Confianza:** Cada certificado está respaldado por una CA superior, y su validez se comprueba hasta llegar a una CA raíz de confianza.

Si el certificado digital es inválido, expirado o revocado, la firma digital no podrá considerarse confiable.

6.4 ¿Qué permite validar los certificados digitales?

Se validan verificando la firma de la autoridad certificadora, la fecha de expiración y listas de revocación. Comprobando varios aspectos esenciales:

- **Firma de la Autoridad Certificadora (CA):** Se verifica que el certificado fue emitido y firmado por una CA confiable y legítima.

- **Fecha de expiración:** Cada certificado tiene una fecha de validez, por lo que se debe comprobar que aún es vigente.
- **Listas de Revocación de Certificados (CRL) o el Protocolo OCSP:** Se consulta si el certificado ha sido revocado por alguna razón (fraude, compromiso de seguridad, etc.).

Este proceso garantiza que solo los certificados digitales válidos y confiables sean utilizados en la verificación de firmas digitales, asegurando la seguridad en transacciones electrónicas, comunicaciones cifradas y documentos digitales protegidos.

6.5 ¿Qué algoritmos se usan para validar los certificados digitales?

Los algoritmos más usados son RSA, ECDSA y funciones hash como SHA-256.

- RSA (Rivest-Shamir-Adleman) : RSA es un algoritmo de cifrado asimétrico ampliamente utilizado para firmas digitales y seguridad en comunicaciones. Fue desarrollado en 1977 por Ron Rivest, Adi Shamir y Leonard Adleman, y se basa en la dificultad de factorizar números primos grandes, lo que lo hace altamente seguro.
- ECDSA (Elliptic Curve Digital Signature Algorithm) :ECDSA (Algoritmo de Firma Digital de Curva Elíptica) es un algoritmo criptográfico basado en criptografía de curva elíptica (ECC). Es una versión más eficiente de DSA (Digital Signature Algorithm) y se usa ampliamente en firmas digitales debido a su alta seguridad y menor tamaño de claves en comparación con RSA.Es más eficiente que RSA porque ofrece la misma seguridad con claves más pequeñas.
- SHA-256, SHA-384, SHA-512 (para la función hash) :Las funciones SHA-2 (Secure Hash Algorithm 2) incluyen SHA-256, SHA-384 y SHA-512 y se usan para garantizar la integridad y autenticidad de los datos. Son ampliamente utilizadas en seguridad informática, criptografía y blockchain.

Ver explicación algoritmos:
Ver RSA, ECDSA y SHA-256

7 Conclusión

Este documento ha sido elaborado siguiendo las recomendaciones del docente y abarcando todos los temas vistos en el curso, con el propósito de consolidar el conocimiento sobre la criptografía asimétrica y su aplicación en sistemas modernos.

A lo largo del desarrollo, se ha demostrado cómo el uso de firmas digitales y certificados juega un papel fundamental en la seguridad de la información, garantizando la autenticidad, integridad y no repudio de los documentos electrónicos. Estas herramientas permiten verificar la identidad del firmante y proteger la información contra modificaciones no autorizadas, asegurando su confiabilidad en entornos digitales.

En un mundo donde la seguridad informática es crítica, aplicar métodos criptográficos robustos no solo es una buena práctica, sino una necesidad para prevenir fraudes, garantizar la privacidad y fortalecer la confianza en las comunicaciones digitales. La correcta implementación de estos mecanismos en sistemas modernos es esencial para proteger los datos en sectores como la banca, el comercio electrónico, las administraciones públicas y cualquier infraestructura tecnológica que maneje información sensible.

Este estudio reafirma la importancia de la criptografía asimétrica como un pilar en la ciberseguridad, incentivando su adopción en el desarrollo de soluciones seguras y resilientes frente a las amenazas actuales.

8 Referencias

References

[1] National Institute of Standards and Technology. (2023). Digital Signature Standard (DSS). Recuperado de `https://www.nist.gov`

[2] Zimmermann, P. (1995). The Official PGP User's Guide. MIT Press.

[3] OpenSSL Foundation. (2024). OpenSSL Cryptography and SSL/TLS Toolkit. Recuperado de `https://www.openssl.org`

[4] Jhon Edison Hincapie (2025) Laboratorio: Firma Digital de un PDF con Kali Linux. Recuperado de https://github.com/jhoney787813/laboratorio_firma_digitales_pfd_kali_linux