Práctica 04.

Certificados digitales

Alvaro Ramírez López

1. Objetivo

- Que el alumno adquiera los conocimientos para identificar los sitios web seguros, mediante los certificados digitales.
- Crear un certificado digital usando OpenSSL

2. Materiales necesarios:

- Equipo de cómputo.
- Sistema operativo Linux.
- Paquetería OpenSSL

3. Datos técnicos:

Firma Digital

El concepto de firma digital fue introducido por Diffie y Hellman en 1976, siendo un mecanismo criptográfico que consiste en un bloque de caracteres que acompaña a un documento acreditando quién es su autor (autenticación) y que no ha existido ninguna manipulación posterior de los datos (integridad). Esta firma digital se emplea con tres objetivos principales:

- Identificar a la persona que ha emitido el mensaje o firmado el documento.
- Garantizar la validez del documento y que éste no ha sido modificado.
- Impedir que el firmante niegue haber firmado el documento.

El proceso de firmado digital se inicia cuando el autor de un documento utiliza su clave secreta dentro del esquema de cifrado asimétrico, a la que sólo él tiene acceso, esto impide que pueda negar su autoría (revocación o no repudio). De esta forma el autor es vinculado al documento de la firma. El software del autor aplica un algoritmo hash sobre el texto a firmar, obteniendo un extracto de longitud fija y absolutamente específico del mensaje. Un cambio mínimo en el mensaje dará lugar a una cadena hash distinta. El extracto tiene una longitud de 128 a 160 bits, dependiendo del algoritmo utilizado, entre los que se encuentran: MD5 o SHA-1. El algoritmo más utilizado en el proceso de cifrado asimétrico es RSA.

Certificado Digital

Un certificado digital es un documento electrónico mediante el cual un tercero confiable (una autoridad de certificación) garantiza la relación entre la identidad de un sujeto o entidad y su clave pública.

Los certificados digitales proporcionan un mecanismo para verificar la autenticidad de programas y documentos obtenidos a través de la red, el envío de correo cifrado o firmado digitalmente, así como el acceso a recursos, etcétera.

La principal diferencia entre la firma digital y el certificado digital es que el certificado sirve para identificar a una persona en la red ante numerosos

Practica 04

Fecha de publicación: 12/11/2024

Correo
Alvaro Ramírez López
alvaro@ciencias.unam.mx

organismos oficiales. El certificado electrónico permite a su poseedor firmar documentos o archivos electrónicamente, es decir, hacer uso de una firma digital segura. Sin embargo, para realizar una firma digital o electrónica no es necesario tener un certificado digital aprobado por una autoridad de certificación.

Dicho de otro modo, el certificado digital permite realizar firmas digitales en internet, pero para realizar firmas digitales en internet no es imprescindible contar con un certificado digital.

En definitiva, las diferencias entre certificado digital y firma digital se resumen en las siguientes:
- El certificado digital se genera a través de una autoridad de certificación que asocia la identidad de una persona al certificado. El proceso requiere un proceso de identificación, autenticación y validación. Por su parte, la firma digital es un código que se crea al firmar el documento, que permite cifrarlo en origen y descifrarlo en destino.
- El certificado digital identifica a su Titular, mientras que la firma digital solo identifica al firmante de un documento o archivo concreto.

Como vemos, la diferencia entre firma digital y certificado digital puede ser difícil de explicar y comprender en primera instancia. La clave es el alcance: mientras la firma digital se refiere a documentos o ficheros concretos, el certificado digital permite identificar a una persona en internet y realizar trámites.

Tipos de certificados

Un certificado SSL es un certificado digital que autentica la identidad de un sitio web y habilita una conexión cifrada. La sigla SSL significa Secure Sockets Layer (Capa de sockets seguros), es un protocolo de seguridad que crea un enlace cifrado entre un servidor web y un navegador web.

Empresas y organizaciones deben agregar este tipo de certificados a sus sitios web para proteger la privacidad y seguridad de sus clientes al momento que estos realizan transacciones en línea.

Para saber si la web es segura, junto a la URL del sitio web se muestra un candado, lo que significa que el sitio web esta protegido y evita que se lea o modifique la información que esta siendo transferida.

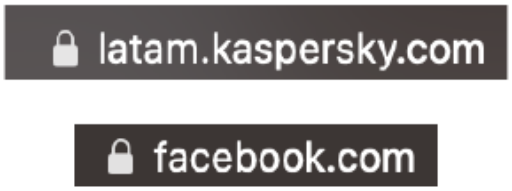
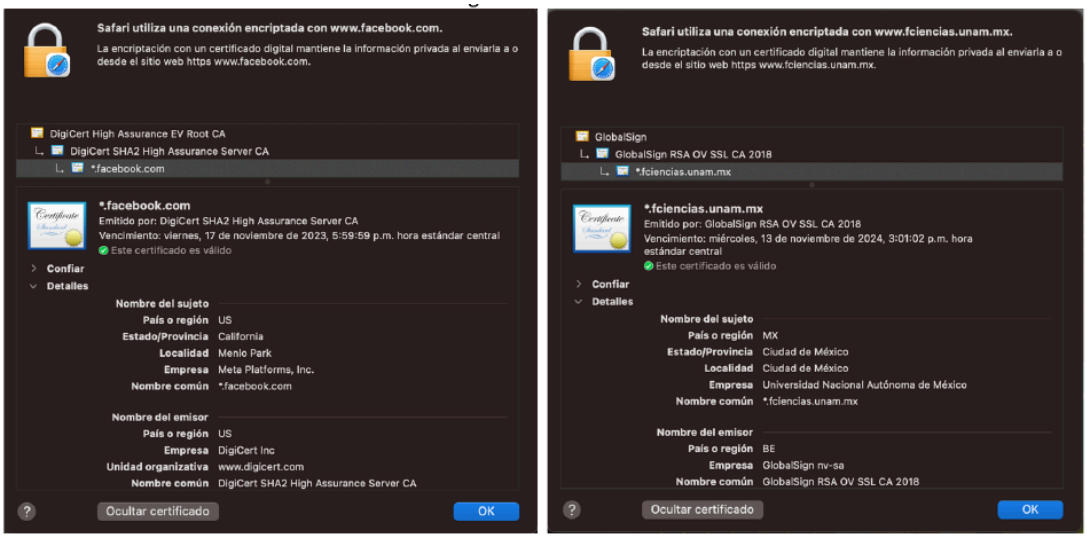


Figura 1: En su navegador web, así se ve que una pagina web tiene un certificado SSL

Al dar clic en el candado se muestran algunos detalles del certificado.



Otra forma de saber si la web esta protegida mediante un certificado SSL es viendo en la URL del sitio web, si aparece como HTTPS (HyperText Transfer Protocol Secure /Protocolo de Transferencia de Hipertexto Seguro), si la web no cuenta con un certificado solo aparecerá con HTTP sin la S de seguro.

Certificados SSL validados por dominio.

Para obtener este tipo de certificado se necesita un proceso de validación mínimo, el propietario del sitio web tiene que demostrar la propiedad del dominio respondiendo un email o llamada telefónica.

Al ser muy fácil de obtener la seguridad será menor y el cifrado mínimo, se usa en blogs o webs informativos, sitios webs en donde no se recopila datos de pagos online, en la barra de navegación solo muestra HTTPS y un candado, sin incluir el nombre de la empresa.

Certificados SSL validados por la organización.

Se expide a empresas, proporcionando un nivel de seguridad mayor al de uno validado por dominio. Para obtenerlo se requiere que información de la empresa sea validad en conjunto con el dominio e información del propietario, en el navegador se activa el candado, https ademas de mostrar la identidad corporativa, mediante cual se puede asegurar que la web es operado por una empresa legitima y no una impostora.

Certificados SSL de validación extendida

Este certificado es el que ofrece un mayor grado de seguridad, pues para obtenerlo se deben seguir un proceso de verificación de identidad exhaustivo y estandarizado a nivel mundial, demostrar los derechos exclusivos de uso del dominio, confirmar la existencia legal, operativa y física, demostrar que se ha autorizado la emisión del certificado, toda la información de identidad es incluida en el certificado.

Este tipo de certificados se usan en webs, aplicaciones donde se recopile datos, procesos de pagos online, inicios de sesión, etc. Por ejemplo bancos, instituciones financieras o grandes marcas, donde al usuario se le garantice una seguridad total al momento de realizar operaciones.

Duración.

Actualmente los certificados SSL tienen una vida útil de 397 días los certificados caducan porque se debe revalidar la información periódicamente y así garantizar que la información para autenticar los servidores y organizaciones sea lo más actualizada y precisa.

Cuando el certificado caduca en la web se muestra un mensaje “Este sitio no es seguro. Existe un riesgo potencial”, si bien el usuario puede acceder, no se recomienda hacerlo pues puede correr el riesgo de recibir un ciberataque.

4. Parte practica

4.1. Crear un certificado digital

1. Instale OpenSSL
2. Cree una carpeta para guardar el programa OpenSSL que será la carpeta de trabajo y acceda a ella.
3. Compruebe que se instaló correctamente OpenSSL.
4. Cree un archivo de texto sin contenido.
5. Aplique una función hash (md5, sha1 o sha265) al archivo anterior y guárdelo en un archivo ∗.bin

Script

```
openssl sha1 -out hash.bin archivo1.txt
```

6. Cree un nuevo archivo de texto con el nombre “archivo2.txt”. En esta ocasión que sí tenga contenido.
7. Ingrese el siguiente comando y explique la función de cada parámetro.

Script

```
openssl enc -des3 -pbkdf2 -in archivo2.txt –out cifra_a.bin -pass pass:12345
```

8. Ingrese el siguiente comando y explique la función de cada parámetro.

Script

```
openssl enc -des3 -pbkdf2 -d -in cifra_a.bin -out descifrado.txt
```

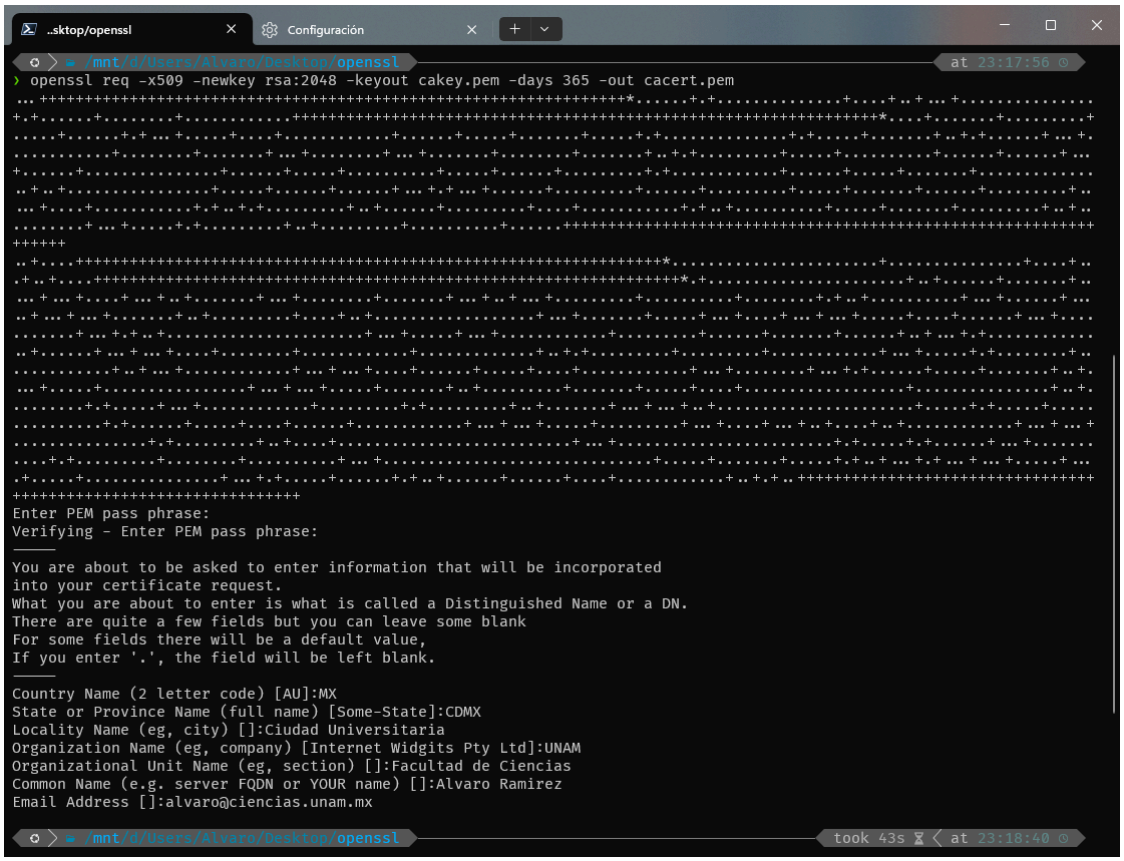
4.2. Crear una Autoridad Certificadora.

1. Se creará una AC para certificados X.509 utilizando el algoritmo de cifrado RSA de 2048 bytes, almacenando llaves públicas y privadas en diferentes archivos.
2. Investigue las características del certificado X.509.
3. Ingrese el siguiente comando y explique cada uno de los parámetros.

Script

```
openssl req -x509 -newkey rsa:2048 -keyout cakey.pem -days 365 -out cacert.pem
```

4. Ingrese una frase contraseña. (Es importante que la recuerde).
5. Complete los datos requeridos con el fin de que sean incorporados en el certificado.



6. Verifique que los archivos de las llaves pública y privada se hayan generado correctamente.

4.3. Generación de certificados

1. El Tipo de certificado a crear es Certificarte Sign Request que puede ser utilizado para dar soporte a sitios Web o sockets. El primer paso es crear la clave privada.

Script

```
openssl genrsa –aes256 –out privkey.pem –passout pass:contraseña
```

2. Verifique que se ha creado el archivo y que tenga el contenido correcto.
3. El siguiente paso es definir al propietario. Se hace una petición donde se especifica a quién pertenece. Se indica la clave privada y la contraseña.

   Ingrese el siguiente comando y explique cada uno de los parámetros.

Script

```
openssl req -new -key privkey.pem -out peticion.pem -passin pass:contraseña
```

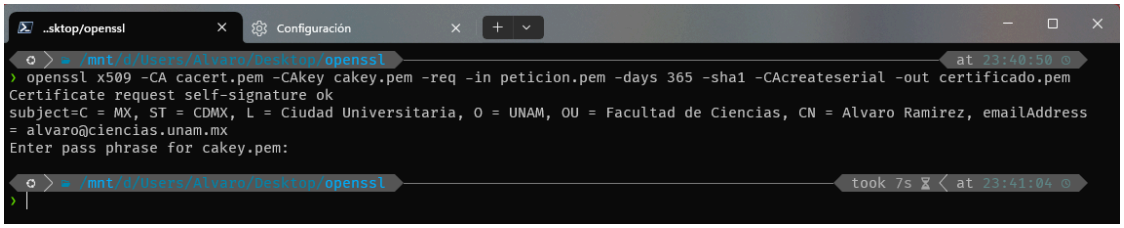
4. Verifique que el nuevo archivo generado sea correcto.

4.4. Firma del Certificado Digital.

1. Ingrese el siguiente comando que genera el certificado firmado por la AC ya creada y explique cada uno de los parámetros.
2. Ingrese la contraseña creada en la **sección 4.2 en el punto 4**

Script

```
openssl x509 –CA cacert.pem –CAkey cakey.pem –req –in peticion.pem –days 365 –sha1 –CAcreateserial –out certificado.pem
```



3. Verifique que se ha creado correctamente el certificado.
4. Ingrese el siguiente comando para obtener información del certificado creado.

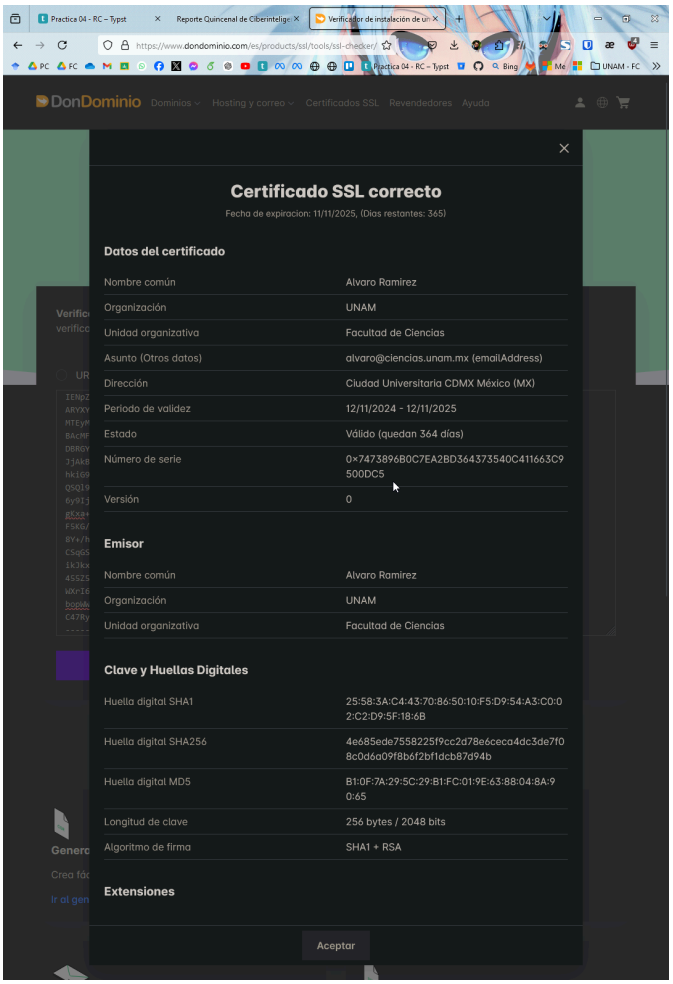
Script

```
openssl x509 –in servidorcert.pem –text –noout
```

5. Explique la información mostrada por el comando anterior.

5. Verificacion de certificado

Entren a la pagina “https://www.dondominio.com/es/products/ssl/tools/ssl-checker/” y peguen en la opcion de texto su archivo `certificado.pem` , les debería aparecer algo así:



6. Entrega

Deberán entregar un reporte en equipo de 4 personas con los siguientes puntos

- El reporte debe de contar con las evidencias del procedimiento desarrollado.
- Las capturas de pantalla a generar son de cada uno de los pasos antes detallados.
- Las conclusiones de la practica deberán de ser una por cada integrante del equipo.

En la entrega deberán de incluir el PEM del certificado así como también todos los archivos generados en el curso de la practica.

Si usan referencias por favor citen todas las fuentes utilizadas, den los créditos de la información que lleguen a utilizar como referencia o crean que les puede ayudar.

Sean cuidadosos en la creación de archivos, identifiquen bien entre llaves públicas y privadas, solicitudes de certificados y hash.

El formato del nombre del PDF seria el siguiente (de la persona que entrega):

Nombre_Apellido.PDF.

Podria verse de la siguiente manera:

Alvaro_Ramirez.PDF

Especifiquen en los comentarios privados del classroom con quien hicieron equipo, sino no habrá calificación para los demás integrantes.