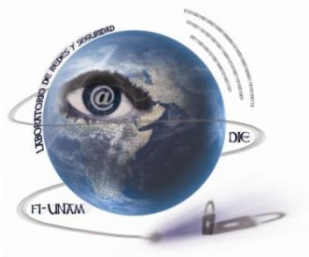




Carátula para entrega de prácticas

Facultad de Ingeniería

Laboratorios de docencia



Laboratorio de Redes y Seguridad

Profesor: Ing. Magdalena Reyes Granados

Asignatura: Laboratorio de Administración de Redes

Grupo: 01

No de Práctica(s): 11

Integrante(s): Gutierrez Silvestre Griselda

Sánchez Bautista Velia


No. de Equipo de cómputo empleado: --

Semestre: 2021-1

Fecha de entrega: 05 de enero de 2021

Observaciones:


CALIFICACIÓN: _____

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	156/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Práctica 11

Mecanismos de Seguridad, Certificados Digitales

Control

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	157/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

1. *Objetivos de Aprendizaje*

- El alumno identificará los diversos tipos de certificados, así como su importancia dentro de los esquemas de seguridad en las redes, utilizando una herramienta de software libre que permite la administración de certificados digitales, OpenSSL

2. *Conceptos teóricos*

El panorama de las telecomunicaciones de datos se ha visto afectado por un gran cambio en los últimos años del siglo XXI. Las innovaciones y cambios tecnológicos suceden con gran velocidad a medida que se perfeccionan y se depuran las ideas y técnicas que han permitido la unión entre la informática, la electrónica y las comunicaciones.

En las transacciones comunes los retos de identificación, autenticación y privacidad son resueltas, con marcas físicas, tales como las firmas. En las transacciones electrónicas, el equivalente a un sello tiene que ser codificado en información. El verificar que el sello se encuentra presente y no ha sido alterado, es la forma en la que el que recibe la información puede confirmar la identidad del que lo envió y de esta manera se asegura que el mensaje no ha sido alterado ni modificado en el camino. Para crear un equivalente electrónico a la seguridad física se usa la llamada criptografía.

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.


Existen varios formatos de certificado digital, los más comúnmente empleados se rigen por el estándar UIT-T X.509v3. El certificado contiene usualmente el nombre de la entidad certificada, un número serial, fecha de expiración, una copia de la clave pública del titular del certificado (utilizada para la verificación de su firma digital) y la firma digital de la autoridad emisora del certificado de forma que el receptor pueda verificar que ésta última ha establecido realmente la asociación.

Para los usuarios, 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.

3. *Equipo y material necesario*

Equipo del Laboratorio:

- PC con sistema operativo Linux, Debian.
- Paquete de instalación de OpenSSL.

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	158/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4. Desarrollo

Modo de trabajar

La práctica se desarrollará en parejas.

4.1 Certificado Digital

Un certificado permite obtener la clave pública de otra entidad ya sea una persona o institución. Se considera como una declaración firmada digitalmente por una entidad indicando que la clave pública de otra persona tiene un valor específico.

Existen diferentes clases de certificados de acuerdo con su utilidad:


- Certificados de servidor, aportan a un sitio Web la característica de seguridad para poder intercambiar información como: números de cuenta, contraseñas, etcétera.
- Certificados para WAP, permiten a los sitios Web la realización de transacciones seguras con sus usuarios móviles. Los certificados WAP permiten mantener conexiones seguras basadas en cifrado y autenticación con dispositivos de telefonía móvil.
- Certificados personales, otorgan seguridad a los correos móviles basados en el estándar S/MIME asegurando que el receptor designado sea el lector del mensaje.
- Certificados para firmar código, permiten a los administradores o desarrolladores de software firmar su código para la distribución segura entre sus clientes.
- Certificados para IPSec-VPN, son los elementos necesarios para que la organización aproveche las cualidades y ventajas del uso de las VPN (Redes Virtuales Privadas - Virtual Network Private).

4.1.1 Instalación de OpenSSL

OpenSSL es una herramienta de software libre desarrollado por los miembros de la comunidad OpenSource que permite la creación y administración de certificados digitales, además de contar con librerías relacionadas con la criptografía, útiles para proporcionar funciones criptográficas, como OpenSSH y navegadores Web (https). Este paquete es importante para cualquiera que esté planeando implementar un cierto nivel de seguridad en una máquina Linux.

4.1.1.1 Abra la aplicación VirtualBox

NOTA: Antes de iniciar la máquina virtual verifique en la opción **Red** que se encuentre marcada la opción **Habilitar adaptador de red->Conectado a: Adaptador puente (Figura No. 1)**.

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	159/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

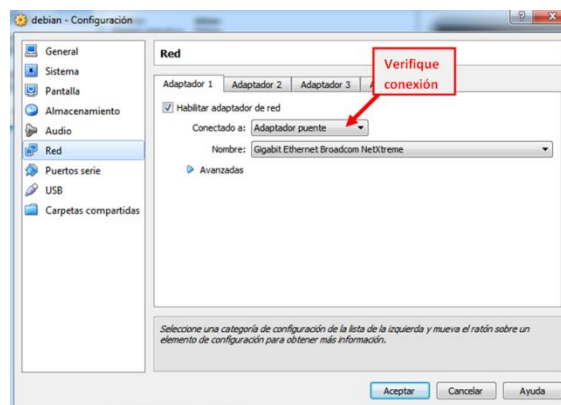


Figura No. 1. Conexión de red.

4.1.1.2 Encienda la máquina virtual

4.1.1.3 Elija la opción de cargar Linux, distribución Debian.

NOTA: En caso de que le aparezca la imagen de instalación (Figura No. 2), dé clic derecho sobre el disco duro. Seleccione la opción que se encuentra palomeada para deseleccionarla, apague la máquina virtual y vuelva a iniciarla.

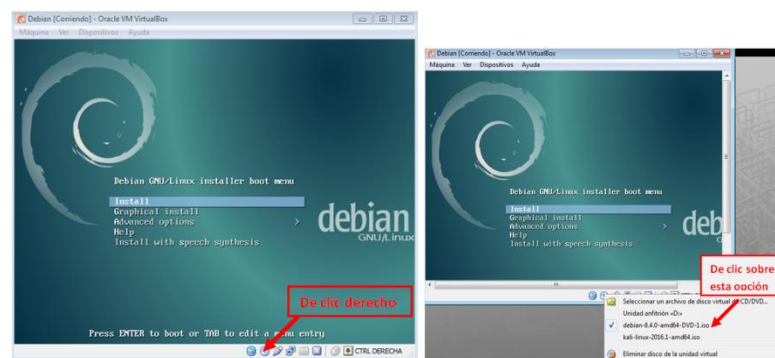



Figura No. 2. Inicio de Máquina Virtual.

4.1.1.4 Inicie sesión en la cuenta de redes.

4.1.1.5 Abra una terminal e ingrese como super usuario, para ello teclee el comando que se muestra a continuación. (Ver Figura No. 3)

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	160/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

NOTA: *su* significa super usuario, por lo que se emplea la misma contraseña de root
redes@debian:~\$ su

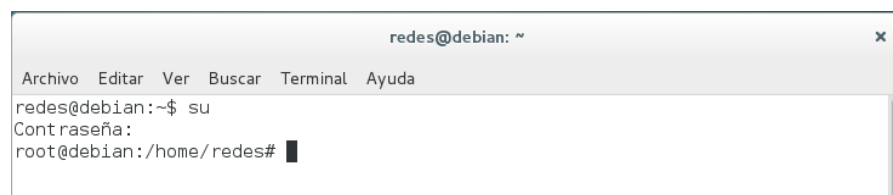


Figura No. 3. Terminal de comandos como root.

4.1.1.6 Cree una carpeta llamada openssl en la carpeta personal del usuario con el cual se registró.

redes@debian:/home/redes# mkdir openssl

4.1.1.7 Ejecute el comando:

redes@debian:/home/redes# apt-get install openssl

Con este comando se instala el servicio de openssl.

4.2 Comandos básicos en OpenSSL

El objetivo de este punto es conocer los comandos básicos de OpenSSL para construir una infraestructura de clave pública.

4.2.1 Abra una terminal de shell, cree una carpeta con el nombre de OpenSSL_iniciales, en el directorio openssl.

NOTA: *iniciales* se sustituirá por el conjunto representativo de letras que decida el equipo


redes@debian:/home/redes# cd openssl
redes@debian:/home/redes/openssl# mkdir OpenSSL_iniciales

4.2.2 Cambie de directorio a **OpenSSLiniciales**, el cual será el directorio de trabajo.

redes@debian:/home/redes/openssl# cd OpenSSL_iniciales

4.2.3 Ejecute el siguiente comando:

redes@debian:/home/redes/openssl/OpenSSL_iniciales# openssl version

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	161/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

I. Anote la versión instalada en el equipo asignado.

OpenSSL 1.0.1t 3 may 2016

4.2.4 Cree un archivo de texto sin contenido alguno (Figura No. 4)

redes@debian:/home/redes/openssl/OpenSSL_iniciales# touch nombre_archivo.txt

4.2.5 Aplique las siguientes funciones hash a un archivo de texto creado en la carpeta de trabajo, y anote el resultado en las siguientes líneas (Figura No. 4).

redes@debian:/home/redes/openssl/OpenSSL_iniciales# openssl md5 nombre_archivo.txt

II. ¿Qué representa la salida del comando anterior?

Representa la huella digital del archivo equipo8_archivo.txt con el algoritmo md5

redes@debian:/home/redes/openssl/OpenSSL_iniciales# openssl sha1 nombre_archivo.txt

III. ¿Qué representa la salida del comando anterior?


Nos representa la huella digital del archivo equipo8_archivo.txt con el algoritmo sha1

IV. ¿Qué diferencias hay al ejecutar el comando con SHA1 y MD5?

Md5 es uno de los métodos de encriptación más usados, no es tan nuevo como sha1, éste regresa un número hexadecimal de 32 caracteres, en modo formato binario 16. En cambio sha1 regresa un número hexadecimal de 40 caracteres, en modo formato binario 20. Sha1 es más fuerte ante ataques de fuerza bruta, y md5 ya ha sido comprometido como método de encriptación por lo tanto es mas vulnerable
redes@debian:/home/redes/openssl/OpenSSL_iniciales# openssl sha1 -out hash.bin nombre_archivo.txt

V. ¿Cuál es la diferencia que existe entre el comando openssl sha1 nombre_archivo.txt y el anterior?

La diferencia es que con openssl sha1 -out hash.bin se firmó el archivo equipo8_archivo.txt, es decir, se guarda la huella digital en el archivo binario hash.bin

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	162/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

```

root@debian:/home/redes/openssl/OpenSSL_lab# nano hola.txt
root@debian:/home/redes/openssl/OpenSSL_lab# openssl md5 hola.txt
MD5(hola.txt) = 68b329da9893e34099c7d8ad5cb9c940
root@debian:/home/redes/openssl/OpenSSL_lab# openssl sha1 hola.txt
SHA1(hola.txt) = adc83b19e793491b1c6ea0fd8b46cd9f32e592fc
root@debian:/home/redes/openssl/OpenSSL_lab# openssl sha1 -out hash.bin hola.txt

```

Figura No. 4 Aplicación de las funciones hash

OpenSSL cuenta con librerías que permiten el cifrado de archivos, con diferentes algoritmos.

4.2.6 Cree otro archivo con nombre entrada.txt y teclee algunos datos (Figura No. 5)

redes@debian:/home/redes/openssl/OpenSSL_iniciales# nano entrada.txt

4.2.7 Posteriormente aplique los siguientes comandos (Figura No. 5):

**redes@debian:/home/redes/openssl/OpenSSL_iniciales# openssl enc -des3 -salt -in
entrada.txt -out cifra_a.bin -pass pass:iniciales**

VI. ¿Qué fue lo que realizó con el comando anterior?

Cifró un archivo con triple DES en el modo CBC, la salida se guardo en el archivo binario,
y además se solicita contraseña

**redes@debian:/home/redes/openssl/OpenSSL_iniciales# openssl enc -des-ede3-cbc -d -in
cifra_a.bin -out descifradoa3des.txt**

VII. ¿Qué fue lo que realizó con el comando anterior?


Lo que hizo fué descifrar el archivo con la contraseña y la salida la puso en un archivo txt

```

root@debian:/home/redes/openssl/OpenSSL_lab# nano entrada.txt
root@debian:/home/redes/openssl/OpenSSL_lab# openssl enc -des3 -salt -in entrada
.txt -out cifra_a.bin -pass pass:lab
root@debian:/home/redes/openssl/OpenSSL_lab# openssl enc -des-ede3-cbc -d -in ci
fra_a.bin -out descifradoa3des.txt
enter des-ede3-cbc decryption password:

```

Figura No. 5 Ejecución de comandos

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	163/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.3 Creación de una AC, Autoridad Certificadora

Una AC (Autoridad Certificadora - Certification Authority) es una organización confiable que recibe solicitudes de certificados de entidades, las valida, genera certificados y mantiene la información de su estado.

Entre las principales tareas de una AC encontramos:

- Admisión de certificados.
- Autenticación del sujeto.
- Generación de certificados.
- Distribución de certificados.
- Anulación de certificados.
- Almacenes de datos.

Los certificados digitales proporcionan un mecanismo criptográfico para implementar la autenticación, siendo seguro y escalable para distribuir claves públicas en comunidades grandes.

Para crear un certificado digital en primera instancia se debe realizar una solicitud de certificado a una AC que respalde la información del certificado solicitado. Algunas AC reconocidas son VeriSign, Visa, etcétera, éstas previo pago devuelven certificados firmados por ellas. Para sustituir a dichas AC se creará una propia para firmar los certificados que se generen.

4.3.1 Estando en el directorio de trabajo teclee el siguiente comando. (ver Figura 1.1)

```
redes@debian:/home/redes/openssl/OpenSSL_iniciales# openssl req -x509 -newkey  
rsa:2048 -keyout cakey.pem -days 365 -out cacert.pem
```


El comando anterior crea una AC para certificados X509 con algoritmo de cifrado RSA de 2048 bytes. La opción `-keyout` permite que la clave privada de la AC se almacene en el archivo `cakey.pem` y la clave pública `-out` en el `cacert.pem`.

El formato de certificados X.509, es un estándar del ITU-T, (Internacional Telecommunication - Union-Telecommunication Standardization Sector) y el ISO/IEC (Internacional Standards Organization-International Electrotechnical Commission) publicado en 1988.

4.3.2 Seguidamente se solicita una frase password para la AC, introduzca la palabra: **.r3d3s.** y confirme la frase.

4.3.3 En el país introduzca el código identificador MX.

4.3.4 El siguiente campo solicita el estado o provincia, introduzca Distrito Federal.

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	164/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.3.5 En el nombre de la localización que solicita introduzca Lab Redes y Seguridad.

4.3.6 En el nombre de la organización introduzca UNAM.

4.3.7 En la unidad organizacional introduzca FI.

4.3.8 En el campo del nombre común introduzca su primer nombre y apellido.

4.3.9 Finalmente proporcione su correo electrónico (Figura No. 6).


```

redes@debian: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@debian:/home/redes/openssl/OpenSSL_lab# openssl req -x509 -newkey rsa:2048
-keyout cakey.pem -days 365 -out cacert.pem
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'cakey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:MX
State or Province Name (full name) [Some-State]:CDMX
Locality Name (eg, city) []:Lab
Organization Name (eg, company) [Internet Widgits Pty Ltd]:LAR
Organizational Unit Name (eg, section) []:LAR
Common Name (e.g. server FQDN or YOUR name) []:LabRyS
Email Address []:lab.redyseguridad@gmail.com
root@debian:/home/redes/openssl/OpenSSL_lab#

```

Figura No. 6. Creación de la Autoridad Certificadora

Hasta este punto se ha creado la AC que validará los certificados que se generen durante la práctica.

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	165/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.3.10 Verifique que los archivos que contienen el certificado de la AC y su clave se han creado en el directorio actual, esto a través de los siguientes comandos:

```
redes@debian:/home/redes/openssl/OpenSSL_iniciales# cat cakey.pem
redes@debian:/home/redes/openssl/OpenSSL_iniciales# cat cacert.pem
```

VIII. Investigue en qué consiste el formato pem.

Es un archivo de certificado de correo mejorado de privacidad que se utiliza para transmitir correo electrónico de forma privada. La persona que recibe este correo electrónico puede estar segura de que el mensaje no fue alterado durante su transmisión, no fue mostrado a nadie más y fue enviado por la persona que dice haberlo enviado, codifica binario con base64 para que exista como una cadena ASCII.

4.4 Petición y Generación de certificados

Es posible obtener un certificado digital a través de dos formas:

- Petición on-line, en este tipo regularmente se solicitan certificados personales, para lo cual se requiere de llenar un formulario, enviar alguna documentación y esperar el certificado firmado por la AC.
- Petición postal, resulta óptimo para la obtención de certificados de servidor, siendo una combinación ya que el CSR (Solicitud de Firma de Certificado - Certificate Sign Request) se envía por correo y la documentación se hace llegar por correo.


Un CSR es un archivo que incluye la información necesaria para solicitar un certificado digital.

El objetivo de este punto es generar un CSR después de crear la AC en el punto anterior.

4.4.1 El primer paso para la generación de un certificado digital es la creación de la clave privada del mismo. Teclee el siguiente comando que crea una clave privada con un algoritmo de cifrado RSA de 2048 bytes y se almacena en el archivo priv.pem, con la opción -passout pass: en la cual le indicará la frase privada para la clave privada. (ver Figura No. 8)

```
redes@debian:/home/redes/openssl/OpenSSL_iniciales# openssl genrsa -aes256 -out
priv.pem -passout pass:clave 2048
```

NOTA : clave se sustituye por la clave privada que desee el equipo, puede ser una frase o una palabra.

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	166/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

```

root@debian:/home/redes/openssl/OpenSSL_lab# openssl genrsa -aes256 -out priv.pem
m -passout pass:iniciales 2048
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
root@debian:/home/redes/openssl/OpenSSL_lab# █

```

Figura No. 8. Creación de la clave privada del certificado

4.4.2 Verifique que el archivo priv.pem se haya creado en su home e identifique en su contenido los encabezados.

redes@debian:/home/redes/openssl/OpenSSL_iniciales# cat priv.pem

4.4.3 El segundo paso es realizar una CSR donde se define el propietario del mismo. El siguiente comando hace una petición con el parámetro subj en donde especificamos a quién pertenece el certificado dentro de las comillas separadas por la /. Así mismo, se indica la clave privada que será utilizada con el certificado además de la frase password.

redes@debian:/home/redes/openssl/OpenSSL_iniciales# openssl req -new -subj "/DC=fi-b.unam.mx/OU=LabRedes/CN=fi-b" -key priv.pem -passin pass:clave -out peticion.pem

IX. Investigue los argumentos del parámetro subj.


Le indicamos a quien pertenece el certificado, por eso el uso de comillas, ya que le indicamos cada apartado de identificación del servidor separados por /. Seguido de la clave privada asociada con el comando "-key serv -priv" usando la clave privada

X. Indique el nombre del archivo de salida de este comando y el parámetro que lo genera.

La petición se genera y almacena en peticion.peticion.pem. El parámetro que lo genera es -out

4.4.4 Verifique que el archivo peticion.pem se haya creado en el directorio actual.

redes@debian:/home/redes/openssl/OpenSSL_iniciales# ls

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	167/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.5 Firma del certificado digital

Los certificados permiten que un individuo demuestre que es quien dice ser, ya que está en posesión de la clave secreta asociada a su certificado y únicamente son útiles si existe una AC que los valide, pues si uno mismo se certifica no hay garantía de que la identidad que se muestra sea auténtica.

Un administrador de redes debe ser capaz de verificar que un AC ha emitido un certificado y detectar si un certificado no es válido. Para evitar la falsificación de certificados la entidad certificadora después de autenticar la identidad del sujeto, firma digitalmente el certificado.

4.5.1 Contando con el archivo de configuración, teclee el siguiente comando que genera el certificado firmado por la AC ya creada.

```
redes@debian:/home/redes/openssl/OpenSSL_iniciales# openssl x509 -CA cacert.pem -CAkey
cakey.pem -req -in petition.pem -days 365 -sha1 -CAcreateserial -out servidorcert.pem
```

XII. Investigue el funcionamiento del comando anterior.

Se está emitiendo el certificado cliente , creando un certificado de tipo x509 cuya entidad certificadora se encuentra en cacert.pem, el certificado que se generó tendrá las especificaciones requeridas almacenado en petition.pem. Con la validez de un año, el número del certificado indicado por el parámetro -day


4.5.2 La aplicación solicita el password de la AC que firma el certificado, introduzca el password configurado inicialmente (.r3d3s.), ver Figura No. 9.

```
root@debian:/home/redes/openssl/OpenSSL_lab# openssl x509 -CA cacert.pem -CAkey
cakey.pem -req -in petition.pem -days 365 -sha1 -CAcreateserial -out servidorcer
t.pem
Signature ok
subject=/DC=fi-b.unam.mx/OU=LabRedes/CN=fi-b
Getting CA Private Key
Enter pass phrase for cakey.pem:
root@debian:/home/redes/openssl/OpenSSL_lab# █
```

Figura No. 9. Solicitud de la frase password

4.5.3 Verifique que el certificado se haya creado y analice su contenido. (ver Figura No. 10)

```
redes@debian:/home/redes/openssl/OpenSSL_iniciales# ls
redes@debian:/home/redes/openssl/OpenSSL_iniciales# cat servidorcert.pem
```


	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	169/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

```

root@debian:/home/redes/openssl/OpenSSL_lab# openssl x509 -in servidorcert.pem -
text -noout
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number: 12264684017100878231 (0xaa34e921e9b57197)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=MX, ST=CDMX, L=Lab, O=LAR, OU=LAR, CN=LabRyS/emailAddress=lab.
redyseguridad@gmail.com
        Validity
            Not Before: Jul 24 23:14:14 2017 GMT
            Not After : Jul 24 23:14:14 2018 GMT
        Subject: DC=fi-b.unam.mx, OU=LabRedes, CN=fi-b
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            Public-Key: (2048 bit)
            Modulus:
                00:e6:10:03:c8:5d:bc:40:73:e7:86:46:5d:80:d0:
                61:c1:25:a1:15:7d:88:af:10:30:c5:9b:14:d0:da:
                59:dc:7c:8b:8d:d9:43:c3:3d:ff:44:12:63:57:6f:
                4c:34:e5:c9:cc:6e:4b:9c:38:81:81:36:7e:1e:fc:
                98:fc:06:a5:75:f6:8d:95:13:2a:42:e5:8c:3d:5e:
                e2:71:da:66:a8:04:62:c9:84:77:d9:0b:a7:a3:21:
                d6:35:9b:9d:a8:a9:36:9d:94:2a:64:97:14:3e:58:
                83:15:f1:cf:f6:fc:14:8d:a2:71:12:ba:45:61:90:

```

Figura No. 11. Información del certificado creado

XIII. Indique la información proporcionada por el comando anterior.


Nos muestra el certificado creado con lo siguientes datos: versión, número de serie del certificado, identificador del algoritmo de firma, nombre del emisor, periodo de validez, nombre del sujeto, algoritmo del clave pública, información de clave pública del sujeto, identificador único del emisor, el módulo, identificador único del sujeto.

4.6 CRL, Listas de Anulación de Certificados

Los certificados tienen un periodo de validez, durante el cual la AC debe mantener la información de las entidades. Entre los datos más importantes que deben ser actualizados se encuentra el estado de anulación del certificado, el cual indica que el periodo de validez ha terminado antes de tiempo y el sistema que lo emplee no debe confiar en él.

XIV. Investigue las razones por las cuales un certificado ya no es válido.

El certificado caducado ha pasado su fecha de validez. Sin certificado de raíz conocida(que no reconoce la autoridad de certificación), el dominio accedido no coincide con el rango válido del dominio en el certificado, una version antigua de protocolo debido a las versiones antiguas de Openssl

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	170/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Las CRL (Listas de Anulación de Certificados - Certification Revocation List) son un mecanismo a través del cual la AC da a conocer y distribuye la información acerca de los certificados anulados a las aplicaciones que los emplean. Estas estructuras de datos firmadas por la AC contienen su fecha y hora de publicación, el nombre de la entidad certificadora y los números de series de los certificados anulados que aún no han expirado.

Un administrador de redes debe obtener la última CRL de la entidad que firma el certificado que emplean sus aplicaciones y verificar que los números de series de sus certificados no estén incluidos en tal lista.

XV. Mencione 2 métodos de actualización de CRL.

Muestreo de CRL's, las aplicaciones acceden a la CA o al almacenamiento de archivos y copian el último CRL a intervalos regulares. Durante el periodo de actualizaciones del CRL podemos aceptar un certificado ya anulado, por lo que el periodo debe de ser corto.

Anuncio de CRL's: la entidad certificadora anuncia un cambio en el CRL a las aplicaciones

El objetivo de este punto es manipular el archivo de configuración de OpenSSL así como los comandos que permiten revocar certificados y generar listas de revocaciones.

4.6.1 Modifique el archivo de configuración openssl.cnf

redes@debian:/home/redes/openssl/OpenSSL_iniciales# nano /etc/ssl/openssl.cnf

y reemplace la línea **dir=../demoCA** por **dir=.**

4.6.2 En el mismo archivo del punto anterior, coloque un signo # para comentar las siguientes líneas:


```
# unique_subject    = no
# crlnumber         = $dir/crlnumber
```

4.6.3 Cree un archivo de nombre index.txt en el directorio de trabajo.

Redes:OpenSSL_iniciales# touch index.txt

4.6.4 Revoque el certificado creado mediante el siguiente comando. (ver Figura No. 12)

redes@debian:/home/redes/openssl/OpenSSL_iniciales# openssl ca -keyfile cakey.pem -cert cacert.pem -revoke servidorcert.pem

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	171/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

```

root@debian:/home/redes/openssl/OpenSSL_lab# openssl ca -keyfile cakey.pem -cert
cacert.pem -revoke servidorcert.pem
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for cakey.pem:
Adding Entry with serial number AA34E921E9B57197 to DB for /DC=fi-b.unam.mx/OU=L
abRedes/CN=fi-b
Revoking Certificate AA34E921E9B57197.
Data Base Updated
root@debian:/home/redes/openssl/OpenSSL_lab#

```

Figura No. 12. Revocando un certificado

Esta operación no modifica el certificado, simplemente actualiza el contenido del archivo de la base de datos index.txt.

XVI. Describa el contenido de dicho archivo.

Se va a la configuración de openssl y revoca el certificado con el id específico, luego actualiza la base de datos

NOTA: La revocación de un certificado no es conocida hasta la publicación de la CRL.

4.6.5 Genere una CRL a través del siguiente comando introduciendo la frase password de la clave privada de la AC (.r3d3s.) (ver Figura No. 13).

redes@debian:/home/redes/openssl/OpenSSL_iniciales# openssl ca -gencrl -keyfile cakey.pem -cert cacert.pem -out ejemplo.crl

```


root@debian:/home/redes/openssl/OpenSSL_lab# openssl ca -gencrl -keyfile cakey.p
em -cert cacert.pem -out ejemplo.crl
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for cakey.pem:

```

Figura No. 13. Creación de una CRL, Lista de Revocación de Certificados

4.6.6 Visualice el contenido del archivo creado en el punto anterior (Figura No. 14).

redes@debian:/home/redes/openssl/OpenSSL_iniciales# cat ejemplo.crl

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	172/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

```

root@debian:/home/redes/openssl/OpenSSL_lab# cat ejemplo.crl
-----BEGIN X509 CRL-----
MIIB6DCB0TANBgkqhkiG9w0BAQsFADCBGzELMAKGA1UEBhMCTVgxDTALBgNVBAgM
BENETVgxDDAKBgNVBACMA0xhYjEMMAoGA1UECgwDTEFSMQwwCgYDVQQLDANMQVIX
DzANBgNVBAMMBkxhYjJ5UzEqMCgGCSqGSIb3DQEJARYbbGF1LnJlZlZlZm1cmk
YWRZ21hWwUy29tFw0xNzA3MjQyMDJhFw0xNzA4MjQyMDJhMBwwGgIJ
AKo06SHptXGFW0xNzA3MjQyMDJhFw0xNzA4MjQyMDJhMBwwGgIJ
cKYFG5HfDi5zBg9f9la0sCwYx6yo2C80sgrz/iBK0oMNQqiYAK+SLYGjdf90BcjU
xJ2muT3pVLUaYd9yJBZkr1F1le1L4gKf4wj9uG18r4/MVyxCTtjlm2X5sgIKpvoJ
UHALNn4s5Ydp8iKE5pB8zpQUEayQ7hPsRZj fFLHRzydAkWDPtG5kvuoLDgfbp5iv
qJDoBYovo3I41m9LVbBEDXySCMKF4ajDqC7LXAE9qh4MxNJN8XomB6LZA8Ut7hL2
M97U0XN7ejEz8Uymq+/1Tl3L9TjZNRGyx892YmrgxwDANK+JDgwZ2Vc1NM7EdZh
Pap8Ig0hAZBZnyPH
-----END X509 CRL-----
root@debian:/home/redes/openssl/OpenSSL_lab#

```

Figura No.14 Contenido del ejemplo ejemplo.crl

4.6.7 Para obtener información acerca de la lista de revocación de certificados, ejecute el siguiente comando y observe que la salida debe ser similar a la Figura No. 15.


redes@debian:/home/redes/openssl/OpenSSL_iniciales# openssl crl -in ejemplo.crl -text -noout

```

root@debian:/home/redes/openssl/OpenSSL_lab# openssl crl -in ejemplo.crl -text -noout
Certificate Revocation List (CRL):
  Version 1 (0x0)
  Signature Algorithm: sha256WithRSAEncryption
  Issuer: /C=MX/ST=CDMX/L=Lab/O=LAR/OU=LAR/CN=LabRyS/emailAddress=lab.redyseguridad@gmail.com
  Last Update: Jul 24 23:46:02 2017 GMT
  Next Update: Aug 23 23:46:02 2017 GMT
Revoked Certificates:
  Serial Number: AA34E921E9B57197
  Revocation Date: Jul 24 23:40:12 2017 GMT
  Signature Algorithm: sha256WithRSAEncryption
  49:48:aa:fd:70:a6:05:1b:91:df:0e:2e:73:06:0f:5f:f6:56:
  b4:b0:2c:18:c7:ac:a8:d8:2f:0e:b2:0a:f3:fe:20:4a:3a:83:
  0d:41:08:98:02:4f:92:2d:81:a3:75:ff:74:05:c8:d4:c4:9d:
  a6:b9:3d:e9:56:55:1a:61:df:72:24:16:64:ae:51:75:95:e9:
  4b:e2:02:9f:e3:08:fd:b8:69:7c:af:8f:cc:57:2c:42:4e:d8:
  e5:9b:65:f9:b2:08:8a:a6:fa:09:52:10:0b:36:7e:2c:e5:87:
  69:f2:22:84:e6:90:7c:ce:94:14:11:ac:90:ee:13:ec:45:98:
  df:14:b1:d1:cf:27:40:91:60:e9:4e:0e:64:be:ea:25:0e:07:
  db:a7:98:af:a8:90:e8:05:8a:2f:a3:72:38:d6:6f:4b:55:b0:
  44:0d:7c:92:08:c2:85:e1:a8:c3:a8:2e:cb:5c:01:3d:aa:1e:
  0c:c4:d2:4d:f1:7a:26:07:a9:59:03:c5:2d:ee:19:76:33:de:
  d4:39:73:7b:7a:31:33:f1:4c:a6:ab:ef:f5:4e:5d:e5:f5:38:
  d9:35:11:b2:c7:cf:76:62:68:2b:83:1c:03:00:d9:3e:24:38:

```

Figura No. 15. Contenido de una CRL, Lista de Revocación de Certificados

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	173/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

XVII. Indique qué significa la salida del comando anterior

Permite revisar certificados revocados de una lista CLR. En este caso nos indica la versión, el algoritmo de encriptación que es el RSA. También muestra la última actualización y la próxima actualización. Además se ve el serial del certificado, así como la clave

En este momento el certificado creado ha sido revocado. El profesor indicará cual es el procedimiento para que los usuarios revisen la validez de los certificados.

5. Conclusiones

Griselda:

Con la realización de la práctica se vieron los pasos para crear un certificado digital y la manera de modificarlo, todo esto empleado openssl.


Velia:

Con la práctica se conoció el procedimiento para crear un certificado digital, para ello se empleo openssl. También, se uso el algoritmo de encriptación RSA.

Referencias:

<https://www.siteground.es/kb/certificado-no-es-de-confianza/>

<https://fsandin.wordpress.com/2009/10/15/crea-tu-propia-entidad-certificadora/>

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	174/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

PRÁCTICA 11
Mecanismos de Seguridad, Certificados Digitales
Cuestionario Previo

1. Investigue en al menos 3 aplicaciones de los certificados digitales.
2. Investigue al menos 2 herramientas adicionales que permitan la administración de certificados.
3. Describa brevemente el funcionamiento básico de un certificado digital.
4. Investigue en qué consiste el estándar ISO 27002.
5. Investigue qué es una CPS (Declaración de Prácticas de Certificación - Certification Practice Statement) dentro de una AC (Autoridad Certificadora).
6. Investigue los elementos del formato de un certificado X.509

```
redes@debian: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
G+RYL/u1MS0h0eWE55IB76DXbI8VP2k+Gj7Na0Tne5Sw4M92ld4v1mXAg1Bmn7Qf  
-----END RSA PRIVATE KEY-----  
root@debian:/home/redes/openssl/OpenSSL_GSGSBV# openssl req -new -subj "/DC=fi-b.unam.mx/OU=LabRedes/CN=fi-b" -key priv.pem -passin pass:clave -out petition.pem  
root@debian:/home/redes/openssl/OpenSSL_GSGSBV# ls  
cacert.pem  cifra_a.bin      entrada.txt      hash.bin        priv.pem  
cakey.pem  descifradoa3des.txt  equipo8_archivo.txt  petition.pem  
root@debian:/home/redes/openssl/OpenSSL_GSGSBV#
```

```
redes@debian: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
root@debian:/home/redes/openssl/OpenSSL_GSGSBV# ls  
cacert.pem  cifra_a.bin      equipo8_archivo.txt  priv.pem  
cacert.srl  descifradoa3des.txt  hash.bin            servidorcert.pem  
cakey.pem  entrada.txt      petition.pem  
root@debian:/home/redes/openssl/OpenSSL_GSGSBV# cat servidorcert.pem  
-----BEGIN CERTIFICATE-----  
MIIDajCCAlCCQD8iHzpveEi5zANBgkqhkiG9w0BAQUFADCBTELMAkGA1UEBhMC  
TVgxGTAXBgNVBAgMEERpc3RyaXRvIEZlZGVyYWwxHjAcBgNVBAcMFUxhYiBSZWRL  
cyB5IFNlZ3VyaWRhZDENMAsgA1UECgwEVU5BTTELMAkGA1UECwwCRkxkGjAYBgNV  
BAMMEUdldGllcnJleIBTYW5jaGV6MSswKQYJKoZIhvcNAQkBFhx2ZWxpYWludnNi  
QGNvbXVuaWRhZC51bmFtLm14MB4XDTEwMDUwNTA4MzIxMVoXDTEwMDUwNTA4MzIx  
MVowQDECMBoGCgmSJomT8ixkARkWDGZpLWIudW5hbS5teDERMA8GA1UECwwITGFi  
UmVkbXZlcnJleIBGNVBAMMBGZpLWIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK  
AoIBAQC+rLbm1uZfJcjl+fttRJerQtlpVU1j0B3617886tW6U0QBYaom+4q3wYo  
zSqvUMUEBdp8+urEvGMRcSxGY4Uyrnl04ZEI7nEaPnir5ZgIA3wnoAN03Aba64K  
QC3nceHT3r1GV/qttw8/bnYEx1U9fPyn0uHGsvInQ6Z9+f0QtPsNshQHISuLYNWKS  
R+vwDVZHFfj1MhuNSUBKwtnbAzHJB0HmYzacssZB01uiCa7GdZYSWyTyNuD25rkW  
EPwMKx0GLcXodi7QmdwYLPQ4NUamBMWU6aF0cG+fnDDX3gIR5UD2u1TyLvoBveFT  
leGaYhzUcJhtRyf53M+UKXiIzfxrAgMBAAEwDQYJKoZIhvcNAQEFBQADggEBAAd8  
HJ2HTFFtYxPpZUaJWSDOKLtkPiqUc7JzFtYvRiVjGF3EJbEggboSDZTYbuEwp3mI  
sACDKSfgXpNb0Lxz2h+llTDWIkr/VH+y7Apqh+/tXHY0ImpuaeV58qKodUJQpae2  
DXPxd+PKUkLYVooUt f77DicQ34TH5DqC3Vgbe0UiZD7Eylud6FQBpGTcy2c1d00S  
CL5cK3P30hQtVH57K6YrEDFGgdqkWj t qzvv0uod9YvPfJ6dw/mdxGvhgz5chWMB  
o yF/bC+9eSf5FfVBIXmPvRpv6EA4m/WaWoNCSHmCuhcWFKWuUsiH5vwJaALIX+j0M  
P38kIL8Uy1NWm3JRyZA=  
-----END CERTIFICATE-----  
root@debian:/home/redes/openssl/OpenSSL_GSGSBV#
```



```
root@debian:/home/redes/openssl/OpenSSL_GSGSBV# openssl crl -in ejemplo
.crl -text -noout
Certificate Revocation List (CRL):
  Version 1 (0x0)
  Signature Algorithm: sha256WithRSAEncryption
  Issuer: /C=MX/ST=Distrito Federal/L=Lab Redes y Seguridad/O=UNAM/OU=FI/CN=Gutierrez Sanchez/emailAddress=veliab.vsb@comunidad.unam.mx
  Last Update: Jan  5 09:20:19 2021 GMT
  Next Update: Feb  4 09:20:19 2021 GMT
Revoked Certificates:
  Serial Number: FC887CE9BDE122E7
  Revocation Date: Jan  5 09:15:25 2021 GMT
  Signature Algorithm: sha256WithRSAEncryption
    6b:6e:a8:f1:3f:94:47:df:23:82:fe:e7:4e:3b:13:10:78:64:
    9d:2f:1c:fd:ed:9d:e7:5d:5d:bf:17:c6:b7:eb:7f:46:53:a9:
    92:0e:1f:3b:69:be:06:c3:ba:8a:26:37:c8:b0:11:a2:b0:1d:
    67:b6:72:76:57:21:ff:45:27:53:3c:dd:25:70:4a:c6:b4:13:
    15:20:46:30:f4:cf:97:17:8b:07:ba:be:a5:73:8b:a5:ed:f8:
    e3:8b:0d:77:3a:60:28:06:56:c9:5d:a7:27:7d:1c:cc:89:9f:
    89:47:39:7a:9c:25:e9:01:ea:73:fb:28:31:dd:b5:0f:6a:c1:
    d6:1f:01:1b:9d:00:8b:bf:46:f2:3b:da:bc:8b:29:02:cf:14:
    41:ef:5f:bb:55:3a:4e:ed:23:8f:60:0e:98:42:da:2e:06:e3:
    75:fd:ee:89:d1:23:16:ff:9f:c7:bc:ad:75:38:e4:a8:a1:0b:
    c9:65:b8:7a:81:9a:59:8c:c7:8e:2e:50:17:a4:d7:0f:31:0c:
    14:32:6b:2e:b3:e2:04:9e:2d:45:31:e3:cd:a1:17:a2:38:6d:
    54:cb:0e:f4:b3:69:1a:e7:0c:14:a6:01:78:bb:a0:c7:70:73:
    68:8d:58:cf:9b:19:be:8b:7b:28:2e:4b:a7:0f:3c:b3:06:6b:
    8e:3c:7f:81
root@debian:/home/redes/openssl/OpenSSL_GSGSBV#
```

Archivo Editar Ver Buscar Terminal Ayuda

```
root@debian:/home/redes/openssl/OpenSSL_GSGSBV# openssl x509 -in servidorcert.pem -text -noout
```

Certificate:

Data:

Version: 1 (0x0)

Serial Number:

fc:88:7c:e9:bd:e1:22:e7

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=MX, ST=Distrito Federal, L=Lab Redes y Seguridad, O=UNAM, OU=FI, CN=Gutierrez Sanchez/emailAddress=veliab.vsb@comunidad.unam.mx

Validity

Not Before: Jan 5 08:32:11 2021 GMT

Not After : Jan 5 08:32:11 2022 GMT

Subject: DC=fi-b.unam.mx, OU=LabRedes, CN=fi-b

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

00:ab:f8:b6:e6:d6:e6:45:25:c8:e5:f9:fb:6d:4d:
18:de:ad:0b:65:a5:55:35:8f:40:77:eb:5e:fc:f3:
ab:56:e9:4d:10:05:86:a8:9b:ee:2a:df:06:28:cd:
2a:af:50:cb:84:05:da:7c:fa:ea:c4:bc:63:2b:11:
c4:b1:19:8e:14:ca:b9:e5:3b:86:44:23:b9:c4:68:
f9:e2:af:96:60:20:0d:f0:9e:80:0d:d3:70:1b:6b:
ae:0a:40:2d:e7:71:e1:d3:de:b9:46:57:fa:ad:c3:
cf:db:9d:81:31:d5:4f:5f:3f:29:f4:b8:71:ac:bc:
89:d0:e9:9f:7e:7f:44:2d:3e:c3:6c:85:01:c8:4a:
e9:58:35:62:92:47:eb:f0:0d:56:47:15:f8:f5:32:
1b:8d:49:40:4a:5a:d9:db:03:31:c9:07:41:e6:63:
36:9c:b1:26:41:3b:5b:a2:09:ae:c6:75:96:12:5b: