Certificados Digitales para servidores web

Francesc Burrull i Mestres

29 de marzo de 2011

Índice

Certificados Digitales para servidores web

1. Objetivos

Los objetivos de la práctica son aprender a configurar el servidor apache con certificados digitales para servir páginas web seguras y la generación de certificados digitales mediante la aplicación *openssl*. Esta práctica está diseñada a modo de "tutorial".

2. Materiales

PC con conexión a Internet y Ubuntu Live CD versión 10.10

3. Procedimiento

3.1. Arranque de linux

1. Arrancar el PC con el live CD de Ubuntu (Ubuntu 10.10) proporcionado. Modificar la secuencia de arranque de la bios si fuese necesario.
2. Seleccionar el idioma "Español" en la pantalla de bienvenida.
3. A continuación apretar el botón "Probar ubuntu" (**sin instalarlo en el PC**). Si se usa un PC del laboratorio la conexión a Internet ya estará configurada, debido a que existe un servidor DHCP en la red.

3.2. Instalación de apache

Una vez haya arrancado el sistema:

1. Abrir una terminal, mediante el menú: Aplicaciones->Accesorios->Terminal
2. Instalar openssl (opcional):

   ```
   ubuntu@ubuntu:~$ sudo apt-get update
   ubuntu@ubuntu:~$ sudo apt-get install openssl
   ```

   El comando *apt-get* es la utilidad que usa Ubuntu para instalar paquetes. El paquete openssl ya viene instalado, pero si se desea se puede actualizar el repositorio de programas e instalar la última versión del paquete *openssl*.
3. Instalar apache2:

   ```
   ubuntu@ubuntu:~$ sudo apt-get install apache2
   ```

El comando *apt-get* es la utilidad que usa Ubuntu para instalar paquetes. Instalaremos el servidor web apache (apache2).

4. Abrir el navegador web firefox y visitar:

   ```
   http://localhost
   ```

   Debería salir la página por defecto. **[1]**

   Obsérvese que si se trata de acceder al web seguro mediante:

   ```
   https://localhost
   ```

   El navegador devuelve un mensaje de error, ya que el servidor web aún no está preparado para servir páginas seguras.

5. Habilitar SSL:

   ```
   ubuntu@ubuntu:~$ sudo a2enmod ssl
   ```

   El comando *a2enmod* habilita el módulo SSL del servidor apache.

   ```
   ubuntu@ubuntu:~$ sudo a2ensite default-ssl
   ```

   El comando *a2ensite* prepara la configuración de la página segura por defecto. Dicha configuración se encuentra en: **[2]**

   ```
   /etc/apache2/sites-available/default-ssl
   ```

6. Reiniciar apache.

   ```
   ubuntu@ubuntu:~$ sudo /etc/init.d/apache2 restart
   ```

7. Visualizar la página segura

   Usando de nuevo firefox: **[3]**

   ```
   https://localhost
   ```

   Ahora se debería poder visualizar la página por defecto segura. El navegador nos advierte que estamos visitando una página que no es de confianza (certificado auto-firmado). Abrir la lista expandible "Comprendo los riesgos" y hacer clic en el botón "Agregar excepción...". A continuación visualizar el certificado. Obsérvese que este certificado es el que lleva la distribución ubuntu por defecto. NO GUARDAR DE FORMA PERMANENTE ESTA EXCEPCIÓN y seleccionar "Confirmar excepción de seguridad".

   Se debería ver la misma página por defecto, pero esta vez segura. Obsérvese la barra del navegador, zona de color azul, donde se puede ver que hemos aceptado esta página como excepción. **[4]**

3.3. Gestión de claves con openssl

El servidor apache ya está funcionando en modo seguro. Ahora bien, las claves que éste utiliza son las que la distribución Ubuntu pone por defecto. Con la aplicación *openssl* se generarán las claves necesarias para autenticar el servidor adecuadamente.

1. Generación de claves:

   A continuación hay que generar todas las claves necesarias.

   a) Clave privada: **[5]**

   ```
   ubuntu@ubuntu:~$ openssl genrsa \
   -out miclaveprivada.pem 1024
   ```

   Alternativamente, si se quiere proteger la clave con una contraseña, utilizar:

   ```
   ubuntu@ubuntu:~$ openssl genrsa -des3 \
   -out miclaveprivadaconpassword.pem 1024
   ```

   usar para la práctica la contraseña: *mysuperpassword*

   b) Certificado:

   ```
   ubuntu@ubuntu:~$ openssl req -new -x509 \
   -key miclaveprivada.pem -out micertificado.pem \
   -days 365
   ```

   Nos preguntarán por:

   - (Si la clave está protegida, contraseña para la clave privada: *mysuperpassword*)
   - Country Name (2 letter code) [AU]:ES
   - State or Province Name (full name) [Some-State]:Murcia
   - Locality Name (eg, city) []:Cartagena
   - Organization Name (eg, company) [Internet Widgits Pty Ltd]:UPCT
   - Organizational Unit Name (eg, section) []:IT1
   - Common Name (eg, YOUR name) []:localhost
   - Email Address []:mi@correo.es

   Ahora tenemos 2 nuevos ficheros, *miclaveprivada.pem* y *micertificado.pem*, donde hay respectivamente la clave privada y el certificado. Se puede ver el contenido del certificado mediante: **[6]**

   ```
   ubuntu@ubuntu:~$ openssl x509 -text -in micertificado.pem
   ```

2. Prueba de las nuevas claves:

   Editar el fichero de configuración de la página segura por defecto.

```
ubuntu@ubuntu:~$
sudo nano /etc/apache2/sites-enabled/default-ssl
```

Alternativamente se puede instalar el editor *vim*, que lleva la sintaxis incorporada resultando en una edición muy cómoda:

```
ubuntu@ubuntu:~$
sudo apt-get install vim
sudo vi /etc/apache2/sites-enabled/default-ssl
```

Sustituir la línea:

```
SSLCertificateFile /etc/ssl/certs/ssl-cert-snakeoil.pem
```

Por:

```
SSLCertificateFile /home/ubuntu/micertificado.pem
```

Y la línea:

```
SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key
```

Por:

```
SSLCertificateKeyFile /home/ubuntu/miclaveprivada.pem
```

Reiniciar apache. Observar que pedirá la contraseña de la clave privada (en el caso de que se la haya puesto y se use miclaveprivadaconpassword.pem).

```
ubuntu@ubuntu:~$ sudo /etc/init.d/apache2 restart
```

Usando de nuevo firefox:

```
https://localhost
```

El navegador advierte que se está visitando una página que no es de confianza (certificado auto-firmado). Abrir la lista expandible "Comprendo los riesgos" y hacer clic en el botón "Agregar excepción...". A continuación visualizar el certificado. Obsérvese que este certificado es el que se acaba de generar. NO GUARDAR DE FORMA PERMANENTE ESTA EXCEPCIÓN y seleccionar "Confirmar excepción de seguridad".

Se debería ver la misma página por defecto, pero esta vez segura. Obsérvese la barra del navegador, zona de color azul, donde de nuevo se puede ver que se ha aceptado esta página como excepción.

Esta situación es similar a la anterior: Se está usando un certificado autofirmado, con la diferencia que éste se acaba de crear (el usado anteriormente era el de fábrica). Esto puede observarse en la zona de color azul de la barra de direcciones del navegador.

3. Crear una Autoridad de Certificación para firmar certificados:

   Si se desea que el navegador acepte sin más un certificado habrá que tomar alguna de las siguientes opciones:

Opción1 Decirle al navegador que almacene de forma permanente la excepción.

Opción2 Usar un certificado expedido por una Autoridad Certificadora que el navegador acepte de fábrica. Suelen costar dinero. Para ver las que el navegador acepta, ver:

Editar -> Preferencias -> Avanzadas (botón) -> cifrado (pestaña) -> Ver certificados (botón)

Estos certificados se consiguen generando una solicitud de certificado:

```
ubuntu@ubuntu:~$ openssl req -new
-key miclaveprivada.pem -out misolicituddefirma.csr
```

Nos pedirán:

- Country Name (2 letter code) [AU]:ES
- State or Province Name (full name) [Some-State]:Murcia
- Locality Name (eg, city) []:Cartagena
  - Organization Name (eg, company) [Internet Widgits Pty Ltd]:UPCT
  - Organizational Unit Name (eg, section) []:IT1
  - Common Name (eg, YOUR name) []:localhost (aquí suele ir el FQDN)
  - Email Address []:mi@correo.es
  - Please enter the following 'extra' attributes to be sent with your certificate request
  - A challenge password []:
  - An optional company name []:

Observar que las opciones por defecto son las mismas que se ofrecían en el punto $1b$. **[7]**

A continuación se enviaría la nueva solicitud de certificado a la Autoridad Certificadora deseada ($$$) ...

Opción3 Crear una Autoridad Certificadora propia, firmar la solicitud anterior e instalar el nuevo certificado en apache y la nueva Autoridad Certificadora en el navegador.

a) Servidor web

Para crear una Autoridad Certificadora se puede utilizar el script CA.sh (/usr/lib/ssl/misc/CA.sh):

```
ubuntu@ubuntu:~$ /usr/lib/ssl/misc/CA.sh -newca
```

Nos preguntará:

- CA certificate filename (or enter to create) -> Apretar enter
- Enter PEM pass phrase: mipassworddeCA
- Verifying - Enter PEM pass phrase: mipassworddeCA

- Country Name (2 letter code) [AU]:ES
- State or Province Name (full name) [Some-State]:Murcia
- Locality Name (eg, city) []:Cartagena
- Organization Name (eg, company) [Internet Widgits Pty Ltd]:UPCT
- Organizational Unit Name (eg, section) []:Seccion de Firmas
- Common Name (eg, YOUR name) []:Certificator
- Email Address []:firmas@correo.es

Please enter the following 'extra' attributes to be sent with your certificate request:

- A challenge password []:
- An optional company name []:

Using configuration from /usr/lib/ssl/openssl.cnf

- Enter pass phrase for ./demoCA/private/./cakey.pem: *mipassworddeCA*

Alternativamente pueden usarse los comandos: **[8]**

```
ubuntu@ubuntu:~$ mkdir -p demoCA/private
ubuntu@ubuntu:~$ cd demoCA
ubuntu@ubuntu:~/demoCA$ openssl req -x509 -newkey rsa:1024
-keyout private/cakey.pem -days 1095 -out cacert.pem
ubuntu@ubuntu:~/demoCA$ cd ..
```

Se puede ver el nuevo certificado de la Autoridad Certificadora mediante: **[9]**

```
ubuntu@ubuntu:~$ openssl x509 -text -in demoCA/cacert.pem
```

Una vez creada nuestra Autoridad Certificadora (mirar el directorio demoCA), firmar con ella la solicitud de certificado que se iba a mandar a firmar:

```
ubuntu@ubuntu:~$
openssl ca -out micertificadofirmado.pem
-infiles misolicituddefirma.csr
```

Se puede ver el contenido del nuevo certificado (ya firmado por la nueva Autoridad Certificadora) mediante: **[10]**

```
ubuntu@ubuntu:~$ openssl x509 -text -in micertificadofirmado.pem
```

Editar de nuevo el fichero de configuración de la página segura por defecto para instalar el nuevo certificado en apache:

```
ubuntu@ubuntu:~$
sudo nano /etc/apache2/sites-enabled/default-ssl
```

Sustituir la línea:

```
SSLCertificateFile /home/ubuntu/micertificado.pem
```

Por:

```
SSLCertificateFile /home/ubuntu/micertificadofirmado.pem
```

Reiniciar apache:

```
ubuntu@ubuntu:~$ sudo /etc/init.d/apache2 restart
```

a) Navegador

Para instalar nuestra Autoridad Certificadora en el navegador:

- Editar->Preferencias -> Avanzadas (botón) -> cifrado (pestaña) -> Ver certificados (botón) -> Importar...
- Ir a la carpeta demoCA y seleccionar cacert.pem
- Marcar "Este certificado puede identificar sitios web"
- Observar que aparece ya nuestra Autoridad Certificadora (UPCT)

Alternativamente podemos traducir el certificado en formato PEM a formato PKCS#12:

```
ubuntu@ubuntu:~$ openssl pkcs12 -export
-in demoCA/cacert.pem -inkey demoCA/private/cakey.pem
-out certificadoCA.p12
```

Nota: El fichero certificadoCA.p12 puede protegerse con contraseña (si se protege con contraseña habrá que introducirla en el siguiente paso).

Y cargar el certificado en formato PKCS#12 con el navegador:

```
file:///home/ubuntu/certificadoCA.p12
```

Características:

- PEM: utiliza el formato ASCII, pudiéndose visualizar con un editor de texto. PEM se utiliza en la mayoría de herramientas SSL. La clave privada y el certificado van en 2 ficheros separados.
- PKCS#12 (Public-Key Cryptography Standard #12) está muy extendido en navegadores. Tanto la clave privada como el certificado van en un único fichero.

Si revisitamos con el navegador:

```
https://localhost
```

Se debería ver la misma página por defecto, pero esta vez segura. Obsérvese la barra del navegador, zona de color azul, donde se puede ver que la página ha sido verificada por UPCT (nuestra Autoridad Certificadora) sin ningún tipo de advertencia por parte del navegador.

Por fin, el navegador ya confía en nuestro flamante sitio web :-)

4. Cuestionario

1. ¿En que directorio se encuentra la página por defecto del servidor apache [pista: visualizar /etc/apache2/sites-enabled/000-default] ?

   [punto 4 en la página 3]

2. ¿En que directorio se encuentra la página segura por defecto del servidor apache?

   [punto 5 en la página 3]

3. ¿Qué certificado usará por defecto el servidor web apache?

   [punto 7 en la página 3]

4. ¿Quién es el expendedor del cerificado que se está utilizando?

   [punto 7 en la página 3]

5. ¿Cual será la ventaja de no usar contraseña para la clave privada del servidor web?

   [punto 1*a* en la página 4]

6. ¿Quién ha validado el certificado?

   [punto 1*b* en la página 4]

7. ¿Qué fichero habría que editar para cambiar las opciones por defecto?

   [punto 3 en la página 6]

8. ¿Qué 2 ficheros son los importantes de este paso?

   [punto 3 en la página 7]

9. El certificado de la Autoridad Certificadora que se ha generado, ¿Es auto-firmado? ¿Qué puede razonar sobre la confianza en un certificado?

   [punto 3 en la página 7]

10. ¿Quién ha validado el certificado?

    [punto 3 en la página 7]