Práctica 5: Uso de Certificados Digitales con OpenSSL

1. CACert: Descripción

CAcert.org es una Autoridad de certificación administrada por la comunidad que gratuitamente ofrece servicios de certificación de clave pública. Surge como una asociación sin ánimo de lucro en Australia con el objetivo de promover la sensibilización y la educación sobre seguridad informática, específicamente sobre PKI.

Los certificados expedidos pueden usarse para firmar y cifrar correo electrónico, identificar y autorizar usuarios conectados a sitios web y transmitir de forma segura datos en Internet.

Cualquier aplicación que soporte Secure Socket Layer (SSL) puede usar certificados firmados por CAcert, tal como lo puede hacer cualquier aplicación que use certificados X.509, por ejemplo para cifrar o firmar documentos digitalmente.

2. Generar un certificado personal con CACert

La primera parte de la práctica consiste en generar un certificado personal con CACert e instalarlo en el navegador para luego exportarlo.

1. Conéctate a la página de CACert `http://www.cacert.org/` y date de alta en el menú que aparece a la derecha. Tendrs que verificar la cuenta a travs de un enlace que te facilitarn por correo electrnico.

2. Instala en el navegador que estás usando el certificado raíz de CACert y el intermedio. El certificado raíz es necesario para poder validar los certificados emitidos usando esta autoridad certificadora.

3. Comprueba con la huella digital de ambos certificados que se son los certificados correctos.

4. Para generar un certificado personal antes tenemos que iniciar la sesin con los datos de acceso asociados a la cuenta que generaste (direccin de correo electrnico y contrasea).

5. Seleccionamos en el men de la derecha `+ Certificado de cliente->Nuevo`. Seleccionamos agregar la direccin de correo a la que queremos vincular el certificado. Tambin seleccionamos que nos muestre las opciones avanzadas para seleccionar como algoritmo hash las SHA-512. De esta manera el algitmo de firma usado en el certificado es ms robusto. Posteriormente slo debemos aceptar las condiciones del acuerdo y pasar al siguiente paso.

6. Debes seleccionar grado alto para la longitud de la clave y generar la pareja de claves que ser certificada.

7. Selecciona el enlace para instalar el certificado y comprueba si has recibido un correo con un enlace para acceder a la información del certificado publicada por la autoridad de certificación.

8. Comprueba que el certificado generado se ha instalado en el navegador correctamente.
9. Exporta dicho certificado en formato PKCS12 (.PFX).
10. Se puede acceder a la a lista de revocacin de esta autoridad de certificacin visitando el enlace `http://cacert.org/revoke.crl`, aunque lleva mucho tiempo descargar el fichero correspondiente. Muestra la configuración de actualización de dicha lista de revocación en el navegador.

3. Extrayendo información de un certificado con OpenSSL

- Abre la consola de OpenSSL.
- Los ficheros pkcs12 contienen la clave publica y la privada. Convertimos al formato PEM el fichero que contiene tu certificado.

  `pkcs12 -in tucertificado.p12 -out tucertificado.pem -clcerts` (exporta sólo los certificados del cliente no el de la CA). Muestra el contenido del fichero generado y comprueba los elementos que contiene. Se solicita varias veces la contraseña que protege al certificado para acceder a la clave privada y exportarla.
- Muestra en la consola la clave pública contenida en tu certificado `x509 -text -in tucertificado.pem`.
- Extrae la clave pública del certificado.

  ```
  rsa -in tucertificado.pem -out tuclave_publica.pem -pubout
  ```
- Extrae la clave privada del certificado cifrándola con triple des.

  ```
  rsa -in tucertificado.pem -des3 -out tuclaveprivada.pem
  ```
- Firma con la clave privada asociada al certificado generado el fichero DancingMan.txt.

  ```
  dgst -sha1 -sign tucertificado.pem -out DancingManFirmado.sig
  DancingMan.txt
  ```
- Verifica la firma que acabas de generar.

  ```
  dgst -sha1 -verify tucertificado.pem -signature DancingManFirmado.sig
  DancingMan.txt
  ```
- Instala los certificados raíz en una aplicación de correo electrónico (Thunderbird, Outlook, etc.)
- Instala tu certificado en dicha aplicación.
- Configura las opciones de la cuenta de correo para que te permita enviar mensajes firmados y cifrados.

4. Referencias

http://www.youtube.com/watch?v=CMm4SyHtEv8