Práctica: confidencialidad con clave pública en OpenSSL

Seguridad de Sistemas Informáticos

Tercera Práctica

1. Autoridades certificadoras (CA)

Existen múltiples iniciativas que gratuitamente ofrecen servicios de certificación de clave pública (Let's Encrypt). 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 estas autoridades, tal como lo puede hacer cualquier aplicación que use certificados X.509, por ejemplo para cifrar o firmar documentos digitalmente.

En esta práctica generaremos un certificado "personalçon un servicio gratuito que no es una CA.

2. Generar un certificado personal con getaCert

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

1. Conéctate a la página getaCert `https://getacert.com/` y seleccione la opción **Generate self-signed certificate** que aparece en la izquierda. Completa los datos y continúa las instrucciones hasta que puedas descargar el certificado.
2. Instala el certificado en el navegador.
3. Comprueba que el certificado generado se ha instalado en el navegador correctamente.
4. Exporta dicho certificado en formato PKCS12 (.PFX).

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 tuclaveprivada.pem -out DancingManFirmado.sig
  DancingMan.txt
  ```

- Verifica la firma que acabas de generar.

  ```
  dgst -sha1 -verify tuclave_publica.pem -signature DancingManFirmado.sig
  DancingMan.txt
  ```