Práctica 4

Certificados digitales

Introducción

En esta práctica vamos a emplear OpenSSL para gestionar Autoridades de Certificación y certificados X509. El uso y gestión de CAs se hace mediante el comando

```
$> openssl ca
```

El nivel de complejidad es elevado, y se recomienda su uso modificando previamente el archivo `openssl.conf` para fijar de antemano entre otros los valores asociados al DN de la CA raíz y de las subordinadas. Su modificación escapa del alcance de esta práctica, pero recomiendo echar un vistazo al mismo para tener una perspectiva de las posibilidades que incorpora. OpenSSL trae un script perl

```
$> /[ruta]/CA.pl
```

Que facilita la creación de CAs y sus certificados correspondientes, aunque dificulta el cambio de parámetros.
Las solicitudes de certificados se realizan con el comando

```
$> openssl req
```

Estas solicitudes pueden realizarse sobre claves creadas previamente o sobre claves creadas en ese mismo momento. En este último caso sólo pueden crearse certificados asociados

a claves RSA. La firma de certificados puede hacerse con `openssl ca` y con `CA.pl`
Por último, una vez creados los certificados podemos actuar sobre ellos con el comando

```
$> openssl x509
```

Puesto que ya tenéis cierto manejo con OpenSSL no voy a ser más explícito en esta introducción. Leed las páginas de manual en

`https://www.openssl.org/docs/manmaster/man1/`

para localizar la información necesaria.

Tareas a realizar

- (3 puntos) Cread una autoridad certificadora raíz. Mostrad los archivos creados y sus rutas, y los valores de las claves generadas.
- (1 punto) Cread una autoridad certificadora subordinada a la anterior. Mostrad los archivos creados y sus rutas, y los valores de las claves generadas.
- (1,5 puntos) Cread una solicitud de certificado que incluya la generación de claves en la misma. Mostrad los valores junto con el archivo.
- (1,5 puntos) Cread un certificado para la solicitud anterior empleando la CA subordinada. Mostrad el archivo y sus valores.

- (1,5 puntos) Cread una solicitud de certificado para cualquiera de las claves que habéis generado en las prácticas anteriores, excepto las RSA. Mostrad el archivo y el valor de la solicitud.
- (1,5 puntos) Cread un certificado para la solicitud anterior utilizando la CA subordinada. Mostrad el archivo y los valores del certificado.

Si no sois capaces de crear la autoridad subordinada, cread los certificados de usuario con la CA raíz.

NOTA: Debéis entregar un PDF describiendo todas las tareas realizadas, incluyendo en él los archivos empleados y generados. No es necesario enviar dichos archivos, pero debéis conservarlos hasta que salga la evaluación de la práctica por si os son requeridos.