PRÁCTICA 4: Certificados Digitales

Seguridad en la Información
Curso 2018-2019

Lenguajes y Ciencias de la Computación.
ETSI Informática, Universidad de Málaga

EJERCICIO 1: Herramienta XCA

XCA (https://www.hohnstaedt.de/xca/) es una herramienta que permite la creación y gestión de certificados digitales de forma simple y visual. Para su gestión, XCA usa una base de datos (ir a Archivo → Nueva Base de Datos) protegida con una contraseña específica y solicitada por entrada. Esta contraseña no sólo protege la base datos, sino también las claves privadas guardadas en disco. La creación (o carga) de una base de datos es la primera operación que hay que realizar al iniciar el programa.

La aplicación tiene 5 funcionalidades concretas, mostradas en cinco pestañas:

- **CLAVES PRIVADAS – Crear el par de claves privada y pública**, ambas asociadas con los certificados generados. Normalmente las claves se generan al crear los certificados, por lo que esta pestaña no se utiliza.

- **SOLICITUDES DE CERTIFICADO – Crear certificados CSR (Certificate Signing Request)**, necesarios para solicitar certificados firmados a una CA (*Certification Authority*). Al crear el CSR se pueden generar las claves directamente sin necesidad de crearlas con anterioridad. También se puede importar los CSR de otras personas con el fin de generar sus certificados en la pestaña *Certificates*.

- **CERTIFICADOS – Crear Certificados** que directamente se guardan una vez han sido firmados por una CA (antes deben pasar por la opción CSR), o importar certificados creados de otras personas.

- **PLANTILLAS – Definir plantillas** de certificados: CA, HTTPS_SERVER y HTTPS_CLIENT. De esta forma, es posible crear certificados "tipo" (p.ej. certificados utilizables en un servidor web) de forma más sencilla.

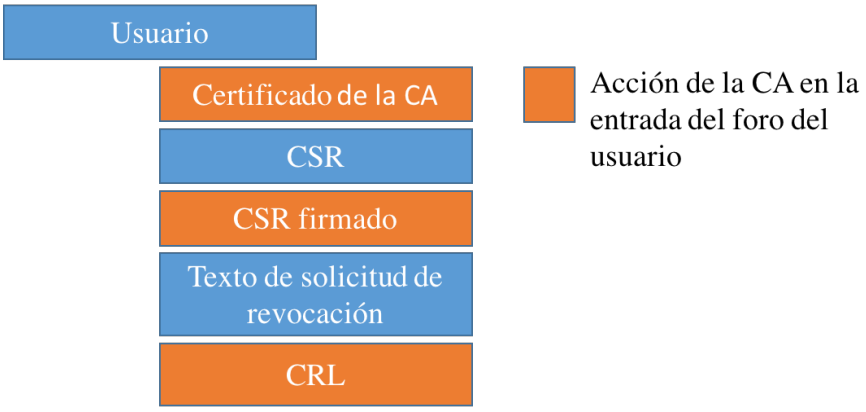
- **LISTAS DE REVOCACIÓN – Gestionar y mantener las CRL**. Cada revocación implica generar una lista de revocación de certificados, y todas las CRL creadas se listarán en *Revocation lists*. También, es posible importar CRL generadas por otras personas.

Teniendo en cuenta estas cuatro funcionalidades de la herramienta XCA, se pide crear en el foro "**XCA**" del Campus Virtual (CV) una entrada (una por cada alumno) con los siguientes puntos:

- *Usuario*. El alumno con rol **usuario** crea un debate en el foro con su nombre y apellidos, e indica su rol de usuario
    - *Certificado de la CA*. El alumno con rol **CA** indica su rol como CA, y adjunta su certificado de CA en formato .crt.
    - *CSR*. El alumno con rol **usuario** adjunta su CSR en formato .pem.

- *CSR Firmado*. El alumno con rol **CA** le devuelve al usuario el CSR firmado (incluyendo el certificado del alumno), todo en formato .p12.
- *Texto de solicitud de revocación*. El alumno con rol **usuario** le pide al CA que revoque su certificado.
- *CRL*. El alumno con rol **CA** adjunta la CRL en formato .pem.

De forma gráfica, la entrada en el foro tiene los siguientes puntos:



La tarea debe realizarse en **pareja**, donde uno actuará de **usuario/sujeto** y el otro de **CA**, invirtiéndose más tarde, los roles (**obligatorio**).

Concretamente, se debe realizar los siguientes pasos según el rol que tenga el alumno:

ROL 1: CA/EMISOR

1. **Crear una CA**. Desde la pestaña de *Certificates*, hay que crear un **certificado auto-firmado**, con unas determinadas características.

   En la pestaña *Origen*, seleccionar la plantilla CA y pulsar en "Aplicar todo". En la segunda pestaña, (*Sujeto*), rellenar los campos *Nombre interno* y *commonName* usando vuestro nombre y apellidos y los caracteres "CA" al final. Antes de finalizar la operación, es fundamental crear una clave privada ("Generar una nueva clave"), y activar la opción "Critical" en la pestaña *Uso de la Clave*, junto con todos los servicios a realizar con la clave (X509v3 Key Usage).

   Una vez creado, hacer público el certificado en el foro (en formato .crt) para que el usuario lo pueda descargar.

   <Pausa: el usuario debe enviar al foro XCA su CSR>

2. **Crear un certificado a partir de un CSR**. Descargar del Campus Virtual el CSR del compañero en formato .pem, importándolo a la herramienta XCA (es importante importar desde la pestaña *Solicitudes de certificado*) para firmarlo. Para ello, es necesario pulsar con el botón derecho el CSR importado y seleccionar la opción "firma". Una vez finalizado el proceso, comprobar que ha sido correctamente firmado.

3. **Exportar el certificado creado**. Tras firmar el CSR, se habrá creado en la pestaña de *Certificates* el certificado del usuario, que debería estar colgando del certificado de la autoridad. Hay que exportarlo y subirlo al Campus Virtual para que el usuario solicitante lo pueda descargar.

   Para la exportación del certificado es necesario exportarlo desde la pestaña *Certificate* y en formato PKCS#12 (p12), indicando una contraseña. La contraseña será 1234.

<Pausa: el usuario debe solicitar la revocación de su certificado>

4. **Revocar un certificado solicitado**. Para la revocación de un certificado, pulsar con el botón derecho sobre ese certificado, y seleccionar la opción "*Revocar*". Rellenar los campos pedidos, y aceptar.

5. **Generar la CRL**. En la pestaña *Listas de Revocación*, crear una "*Nueva CRL*". Observar las opciones, y aceptar.

6. **Exportar la CRL**. Tras el último paso, se habrá creado una CRL. Es necesario exportar dicha CRL en formato .pem, y subirla al CV para que el usuario pueda comprobar que su certificado ya está revocado.

ROL 2: USUARIO/SUJETO

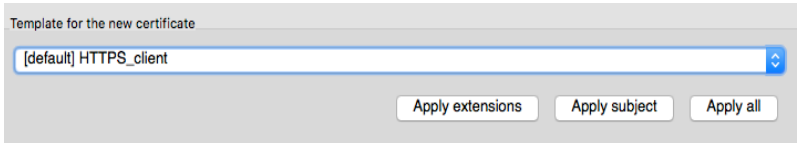
<Nota: la CA debe haber actuado ANTES, exportando su certificado autofirmado al CV >

1. **Importar el certificado de la CA** en la pestaña *Certificates*.

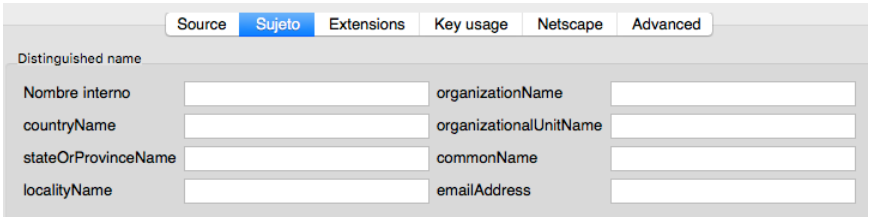
<La CA debe esperar hasta que el usuario haya hecho el punto 3 del ROL 2>

2. **Crear un certificado CSR**. Hay que crear un CSR (*Certificate Signing Request*) desde la pestaña *Solicitudes de Certificado*, con unas determinadas características.

   Primero, en la pestaña *Origen*, seleccionar la plantilla HTTPS-client, y pulsar el el botón "Aplicar Todo".



   Posteriormente, en la pestaña *Sujeto*, rellenar los campos relacionados con el usuario, y al menos aquellos relacionados con el *Nombre interno* y el *commonName*. En el *commonName* es esencial poner el nombre real del alumno para luego identificar el certificado.



Por último, generar las claves (botón "Generar una nueva clave"), y el certificado.

3. Una vez creado el CSR, **exportar el CSR** en formato PEM (es un certificado con codificación ASCII (no legible) utilizado para autenticar a un sitio web seguro) y enviar dicho documento a la CA a través del Campus Virtual.

   <Pausa: la CA debe actuar>

4. Cuando la CA haya creado el certificado solicitado, debemos **importar dicho certificado** a la herramienta XCA. Para ello, en la pestaña Certificados, usaremos el botón "Importar P12"; y tras introducir la contraseña (1234), pulsaremos el botón "Importar todos".

5. Solicitar a la CA (a través de un mensaje de texto) la **revocación del certificado**.

   <Pausa: la CA debe actuar>

6. **Importar la CRL** firmada por la CA en la pestaña *Listas de Revocación*. Una vez importado, el sistema actualizará el estado del certificado, marcándolo como no confiable.