PRÁCTICA 4: Certificados Digitales

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

EJERCICIO 1: Crear certificados digitales con 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.

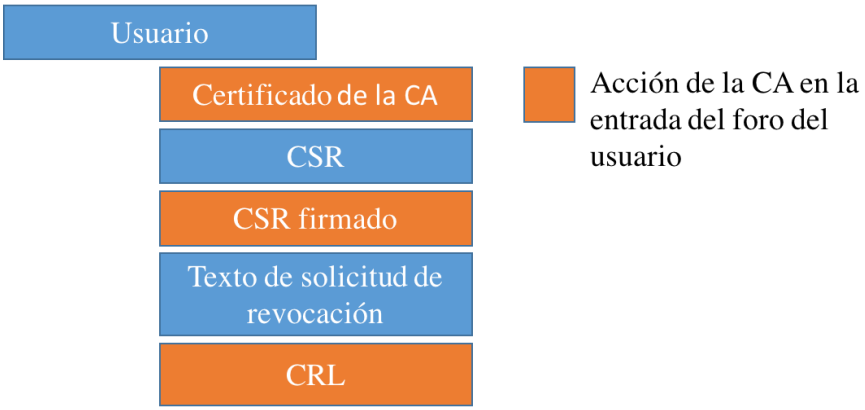
- **LISTAS DE REVOCACIÓN – Gestionar y mantener las CRL**. Cada revocación implica generar una lista de revocación de certificados, y todas las CRL creadas se listarán en *Revocation lists*. También, es posible importar CRL generadas por otras personas.

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). En esta entrada el alumno tomará dos roles: **usuario** y **CA**, y realizará las siguientes tareas:

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

- (Rol **CA**) *CSR Firmado*. El alumno adjunta el CSR firmado (es decir, el certificado del alumno) en formato .crt.
- (Rol **usuario**) *Texto de solicitud de revocación*. El alumno pide a la CA que revoque su certificado ("Revoca el certificado, me han robado la clave").
- (Rol **CA**) *CRL*. El alumno adjunta la CRL en formato .pem.

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



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

1. (Rol **usuario**) **Usuario**. Como se ha mencionado, el alumno crea un debate en el foro con su nombre y apellidos, e indica su rol de usuario ("Hola, soy usuario"). No hay que hacer operaciones en el programa XCA.

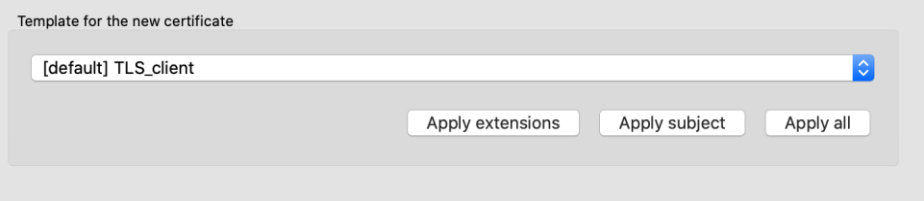
2. (Rol **CA**) **Certificado de la CA**. Desde la pestaña de *Certificates (Certificados)*, hay que crear un nuevo **certificado auto-firmado**, con unas determinadas características.

   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).

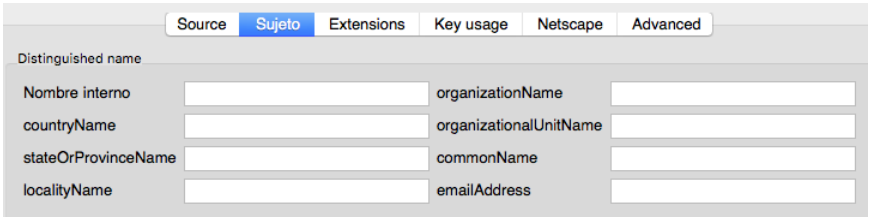
   Una vez creado, **hacer público el certificado en el foro** (en formato .crt).

3. (Rol **usuario**) **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 TLS_client (en algunas versiones antiguas puede aparecer HTTPS_client), y pulsar 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.

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.

4. (Rol **CA**) **CSR Firmado**. Para generar el certificado utilizando el CSR, es necesario pulsar con el botón derecho el CSR creado en el paso 3, y seleccionar la opción "firma". Tras indicar que debe usarse el certificado de la CA para firmar el CSR (pestaña Origen), ya puede crearse el certificado.

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

   Para la exportación del certificado es necesario exportarlo desde la pestaña *Certificate* y en formato .crt.

5. (Rol **usuario**) **Texto de solicitud de revocación**. El alumno pide en un mensaje al CA que revoque su certificado a través del foro. No se realiza ninguna operación en XCA.

6. (Rol **CA**) **Revoca un certificado y crear la CRL**. Para la revocación de un certificado, pulsar con el botón derecho sobre ese certificado, y seleccionar la opción "*Revocar*". Rellenar los campos pedidos (p.ej. revocación por compromiso de la clave), y aceptar.

Para generar la CRL: En la pestaña *Listas de Revocación*, crear una "*Nueva CRL*". Observar las opciones, y aceptar.

Para **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 profesor pueda comprobar que el certificado ha sido revocado.

EJERCICIO 2: Cadena de confianza

Crear con XCA un certificado de usuario emitido por una autoridad que establezca una cadena de confianza con otra autoridad (CA-1-Nombre-Apellidos y CA-11-Nombre-Apellidos). El certificado de usuario deberá permitir posteriormente firmar un documento PDF con el certificado resultante. El documento deberá contener:

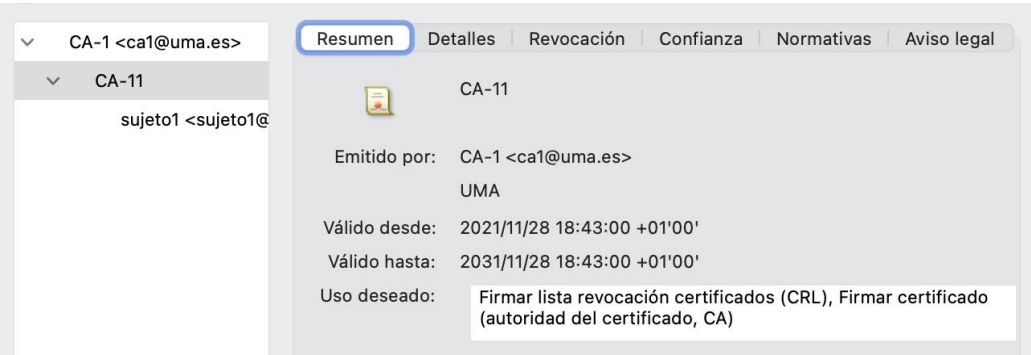
- Nombre
- Apellidos
- Fecha de creación
- Captura de pantalla de XCA mostrando las extensiones del certificado de usuario.
- Firma digital

La cadena de confianza deberá seguir el siguiente patrón:

- Sujeto-Nombre-Apellidos del alumno/a cuyo certificado esté firmado por la autoridad CA-11.
- CA-11-Nombre-Apellidos del alumno/a, cuyo certificado esté firmado por CA-1.
- CA-1-Nombre-Apellidos del alumno/a.

El certificado de usuario (alumno/a) deberá permitir únicamente firmar digitalmente documentos y no otros usos.

Comprueba en el propio lector de PDF Adobe que, efectivamente, existe una firma digital asociada al documento (ver figura a continuación), donde hay una jerarquía de autoridades (CA-1 > CA-11) y finalmente el certificado del sujeto (con los datos del alumno/a).



EJERCICIO 3: SMIME

Crear una CA capaz de emitir certificados y mediante esa autoridad crear un certificado de usuario final con sus datos reales:

- Nombre y apellidos
- Dirección de email

Se deberá poner atención cuando se generan los certificados digitales en el XCA, dejando claro su utilidad para SMIME. Todos los certificados deberán ser instalados en el gestor de correo electrónico Thunderbird (https://www.thunderbird.net/es-ES/).

Una vez hecho esto, se compartirán los certificados correspondientes con algún compañero/a y a continuación se enviará un correo cifrado y firmado electrónicamente. El receptor del correo electrónico deberá comprobar que efectivamente los mensajes están debidamente protegidos.

Repetir la misma operación en el sentido contrario de la comunicación.

NOTA 1: La configuración del correo UMA con el gestor de correo electrónico Thunderbird puede consultarse aquí: http://u.uma.es/b1L/ConfigCorreo/

NOTA 2: Durante la configuración del correo UMA, **debe** configurarse el servidor como IMAP, manteniendo los correos en el servidor. Si no se realiza esta configuración, el gestor de correo electrónico *bajará todos los mensajes y los borrará del servidor*.