Planteamiento

El uso de la criptografía de clave pública como herramienta de identificación a través de la firma digital tiene la limitación de que este protocolo sólo identifica a una clave, no a una entidad física concreta. Este último paso, sólo se puede hacer a través de una infraestructura de clave pública (PKI). El primer principio de funcionamiento de esta infraestructura es la confianza. Una persona que vaya a utilizar las comunicaciones digitales debe establecer una confianza inicial en alguien A; para posteriormente trasladar esa confianza a través de las entidades en las que confía A. Una entidad en la que se pueda confiar va a ser una Autoridad de Certificación (CA) y su labor será la de certificar la identidad de sus suscriptores por medio de certificados digitales expedidos (firmados) por la CA.

En esta práctica proveeremos de identidad digital a los votantes válidos a través de una PKI. Para ello, generaremos certificados válidos para todos los integrantes de la misma, para finalizar generando tres certificados de votantes para Alicia, Blanca y Carlos, respectivamente.

Comenzaremos descargando la interfaz de creación de certificados XCA (también accesible en Moodle). La instalación tampoco ofrece ningún problema. Esta aplicación nos permite la generación de certificados, sin tener que interactuar directamente con la librería criptográfica TLS.

Configuraremos todos los certificados de la aplicación XCA para que utilice la función Hash SHA-256.

A continuación procederemos a generar una CA que será usada para emitir certificados empleados en la práctica. Para ello emplearemos la aplicación XCA. Empezaremos creando una base de datos de claves tanto secretas como públicas, protegiéndola con un password.

Después, procederemos a la creación de un certificado raíz, donde el firmante y el suscriptor sean la misma entidad en la pestaña Certificates, no olvidando seleccionar CA como plantilla de certificado.

Se nos pedirá una serie de datos para generar el certificado, que pueden ser los siguientes:

CN (Country Name): ES

State or Province: Zaragoza

Locality Name: Zaragoza

Organization Name: Universidad de Zaragoza

Organizational Name: Dep. Tecnico

Common Name: El nombre por el que se va a conocer al CA.

Email Address: Mail para contacto con los dueños de la CA

Una vez establecida la CA como entidad confiable, describiremos cómo se genera un certificado para un servidor. En primer lugar será necesario crear una petición de firma de certificado (CSR o Certificate Signing Request) que luego firmaremos con el certificado de la CA que ya hemos creador. No nos olvidemos de seleccionar correctamente la plantilla de certificado de servidor.

CN (Country Name): ES

State or Province: Zaragoza

Locality Name: Zaragoza

Organization Name: Entidad de confianza

Organizational Unit: Dep. Tecnico

Common Name: localhost (URL de la entidad)

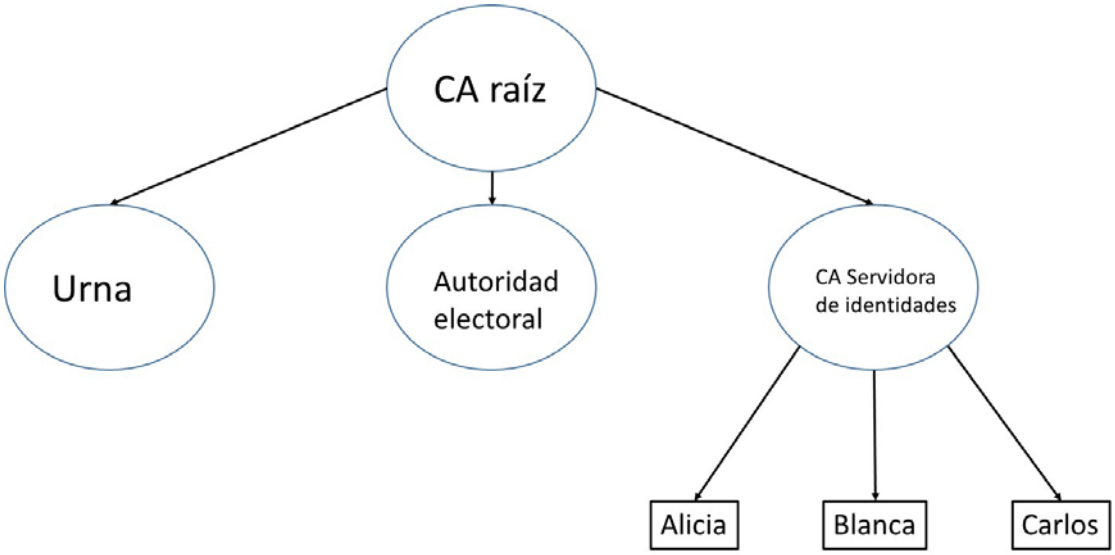
Email Address: Mail para contacto de la entidad

Common Name: El nombre del dominio de nuestra página (es VITAL ponerlo de forma correcta o de lo contrario nuestro certificado no funcionará de forma correcta).

Generar un certificado de usuario, que sería la “hoja” de la PKI arbórea que estamos describiendo, se realizaría de forma análoga a la de un certificado de servidor pero cambiando la plantilla que se va a usar, pulsando “client” en el momento de generación de la CSR y del certificado.

Trabajo a realizar durante la práctica

En esta práctica, una vez nos hayamos familiarizado con el uso de XCA, generaremos todos los certificados necesarios para sustentar la PKI, que tiene este diseño arbóreo.



- Se deberá entregar a través de Moodle dos ficheros:

    a. Un fichero comprimido .zip que contenga todos los certificados necesarios para la infraestructura.

    b. Un fichero .pem conteniendo la clave privada de la CA raíz.