Instrucciones para petición de certificado SSL x509 para servidor web.

El presente documento describe los procesos que se han de realizar a la hora de solicitar un certificado digital para un certificado con un único FQDN y con varios alias.

1.- Generación de las peticiones de certificados o CSR (Certificate signing Request)

Se hará la petición por el sistema de gestión de peticiones CAU mediante el envío por mail junto con la petición del formulario de solicitud del servicio y del archivo CSR.

Deberá tener en cuenta a la hora de preparar el CSR:

- La longitud en bits del certificado o nivel de encriptación debe ser como mínimo de **2048 bits**.
- Únicamente se podrán solicitar certificados dentro del dominio **uned.es***.
- Los campos **C, O y CN** son obligatorios:
    - CN = Nombre del servidor completo o nombre de DNS, debe existir de forma previa.
    - OU = CTU (DIA, LSI, POLI, …).
    - O = Universidad Nacional de Educación a Distancia / UNED
    - L = Madrid
    - S = Madrid
    - C = ES
- Para certificados con varios nombres o alias:
    - No se deben incluir valores en el campo SubjectAltName.
    - El CSR solo ha de incluir el nombre principal del servidor.
    - Adjunte un archivo TXT a la petición, en dicho archivo consigne cada nombre alternativo completo (con el dominio incluido xxx.yyy.uned.es).
    - Refleje dichos nombres en el formulario.
- El CN no puede contener el carácter asterisco.
- Indicar el tipo de servidor (IIS, Apache,…) donde va a quedar instalado el certificado.

* Existe la posibilidad de pedir certificados fuera de este dominio, siempre que se pueda justificar que la titularidad y gestión directa de dicho dominio pertenece a la UNED o a algún organismo relacionado directamente con ella.

2. Métodos de generación.

La mayor parte de los sistemas que utilizan certificados para securizar las comunicaciones, como Internet Information Service, tienen integradas funcionalidades para crear los CSR, busque la información correspondiente a su sistema proporcionada por el fabricante, ya que la cantidad de sistemas y el constante cambio de versiones hacen que no se pueda generar una guía global. En los siguientes puntos de este documento encontrará guías de los sistemas más extendidos a modo de ejemplo.
Puede encontrar guías de creación e instalación de certificados en la siguiente URL:

https://www.digicert.com/security-certificate-support.htm

En todos los procesos **es obligatorio crear la clave privada en el propio servidor** donde se dará el servicio, si existieran indicios de que la clave hubiera podido salir del servidor se entenderá que su seguridad ha podido ser comprometida y se revocará el certificado.

2.1 Servidores Windows para IIS.

Sigua las instrucciones de cómo implementar SSL en IIS:

IIS 8: https://www.digicert.com/csr-creation-microsoft-iis-8.htm

IIS 7: http://technet.microsoft.com/es-es/library/cc732230(v=ws.10).aspx

También puede descargarse el programa OpenSSL para Windows y realizar el mismo proceso que para Linux del siguiente punto.

2.2 Servidores Linux, Mac OSX y otros.

En estas instrucciones se presupone que trabajamos en un ordenador Linux OpenSSL instalado, *y se ha sustituido el openssl.cnf, por este:*

http://portal.uned.es/pls/portal/url/ITEM/DF07D9CEC4561B2FE040660A3370501E

2.2.1. Petición de un certificado SSL con un único nombre.

Necesitamos primero un fichero de datos aleatorios para la entropía, con este comando creamos un fichero rand.dat, con 1024 bytes datos binarios aleatorios**:

openssl rand -out rand.dat 1024

Generamos la que será la llave privada RSA de 2048 bits y el CSR:

*openssl req -new -newkey rsa:2048 -nodes -sha256 -out **FQDN.csr** -keyout **FQDN.key** -subj "/C=ES/ST=28015/L=Madrid/O=UNED/OU=<DEPARTAMENTO>/CN=<FQDN>"*

- Deberá hacer llegar el contenido del fichero NOMBRE.csr al CAU, **nunca él .key**.
  Tenga en cuenta que la clave privada así generada no está protegida por contraseña, algunos sistemas por razones de automatismos desaconsejan el uso de dicha protección, ya que deberá introducirse manualmente cada vez que se vaya a hacer uso de la clave, como por ejemplo al iniciar un servidor web Apache.
  La contraseña puede posteriormente deshabilitarse o habilitarse:
  Habilitarla: openssl rsa -des3 -in your.key -out your.encrypted.key
  Deshabilitarla: openssl rsa -in your.key -out your.open.key

- Si edita el archivo con un editor que trabaje con códigos internos como MS Word puede invalidarse el CSR. La mejor práctica es utilizar el block de notas.

- Para ver el contenido del CSR desde consola: *openssl req -noout -text -in NOMBRE.csr*

** Es recomendable generar un fichero de entropía aleatoría por certificado. Puede emplear otro tamaño de bytes.