Instrucciones para generar el CSR de certificado SSL Multidomain

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

Un mismo certificado puede certificar varios nombres de máquina, llamándose entonces certificado con nombres alternativos de sujeto o SAN.

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

Se hará la petición por el sistema de gestión de peticiones del CAU

Deberá tener en cuenta los siguientes puntos:

- La longitud en bits del certificado o nivel de encriptación debe ser como mínimo de **2048 bits**.
- Nombre FQDN de DNS del servidor principal y otros FQDN. Un mismo certificado puede certificar varios nombres (alias o nombre alternativo).
- Los campos **C, O y CN** son obligatorios, **C=ES, O=UNED y CN= FQDN** Principal
- Los alias se deben incluir valores en el campo SubjectAltName
- El CN no puede contener el carácter asterisco.
- Únicamente se podrán solicitar certificados dentro del dominio **uned.es***
- Si indico que el CTU-UNED generase la clave privada, el formato de entrega será PKCS#12.
- Si indico que el CTU-UNED generase la clave privada deberá indica si se desea que la clave privada este protegida por contraseña.

* 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.- Consideraciones previas.

Deberá rellenar el formulario indicando todos los nombres FQDN a consignar en el certificado. El formulario contempla hasta 10 alias del FQDN principal, si necesitará más, en el formulario puede separar los nombres por comas e incluso no consignar los campos DC del certificado: uned.es, ya que se presupone.

Deberá generar un CSR con un unico nombre de servidor FQDN, y adjuntar en un fichero de texto los demás nombres que desea que lleve el certificado, consignando un nombre por línea, sin comas ni marcas de separación, lños nombres debeán llevar el dominio completo, esto es hasta '.uned.es'

Se harán llegar los tres archivos, solicitud, y archivo de texto con nombres alternativos, junto con el CSR en fichero TXT ** adjunto al email (no HTML) a través del sistema de gestión de peticiones.

En la petición se deberá indicar el tipo de servidor en el que se va a emplear el certificado y el formato.

** El formato del fichero ha de ser modo texto plano, si se ha de editar, utilizar el bloc de notas o algún programa similar que no añada códigos de control ocultos pues invalidarían el CSR.

3. Métodos de generación.

La mayor parte de los sistemas que utilizan certificados para securizar las comunicacione, 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.

3.1 Mediante OpenSSL, recomendado para Linux.

Si desea crear el CSR y la clave privada por que el sistema no tenga capacidad de generarlo, o prefiera crearlo usted, deberá bajarse el paquete de software 'OpenSSL', disponible para diferentes sistemas operativos. Una vez instalado el software, desde una consola deberá ejecutar el siguiente comando para generar el CSR y la clave privada mediante OpenSSL:

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

Sustituya:

<DEPARTAMENTO> por su unidad, ej:; CTU, DIA, INNOVA...

<FQDN> por el nombre DNS donde se de el servicio, ej: www.uned.es, portal.uned.es,...

Tenga en cuenta que la clave privada así generada no esta 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 según las instrucciones que al efecto estarán disponibles en:

https://descargas.uned.es/intranet/pdf/2015-04-08-CTU-SEGURIDAD-MANUS-Instrucciones_certificado_SSL_x509_V1.pdf

3.2 Servidores Windows para IIS.

Sigua las instrucciones de como implementar SSL en IIS:

IIS 6: http://support.microsoft.com/kb/299875/es

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.

4. Metodo alternativo de 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 con cifrado triple DES:

 # openssl genrsa –rand ./rand.dat –des3 2048 > ./NOMBRE.key

De esta llave (NOMBRE.key) generamos la petición o CSR:

 # openssl req –new –config ./openssl.cnf –key ./NOMBRE.key –out ./NOMBRE.csr

Deberá hacer llegar el contenido del fichero NOMBRE.csr al CAU, **nunca él .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 bloc de notas.

Para ver el contenido del CSR desde consola:

 # openssl req -noout -text -in NOMBRE.csr

Para quitarle la contraseña a la clave privada:

 # openssl rsa -in NOMBRE.key -out newNOMBRE.key

** Es recomendable generar un fichero de entropía aleatoría por certificado.